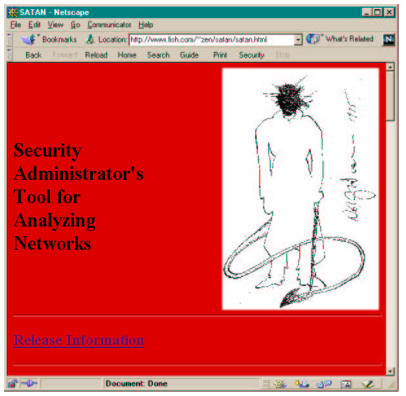
Seguridad en Redes

Agosto'2002

Agenda

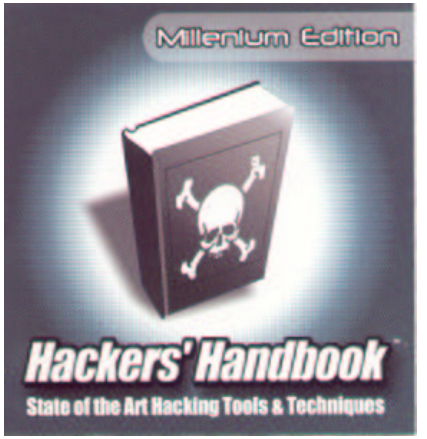
- Introducción
- Ataque
- Técnicas de Seguridad
- Arquitectura de Seguridad
- Tecnologías para Seguridad
- Resumen

Chile : Detenido “Hacker” de sólo 15 años
El Mercurio – Agosto de 2001

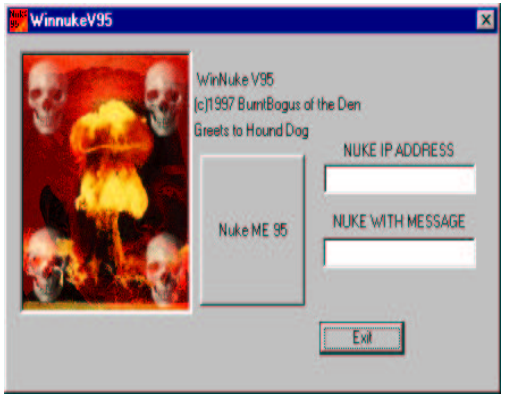


- **Daños y pérdidas por más de $3.000.000**

- **Según investigaciones se trata de personas menores de 30 años**



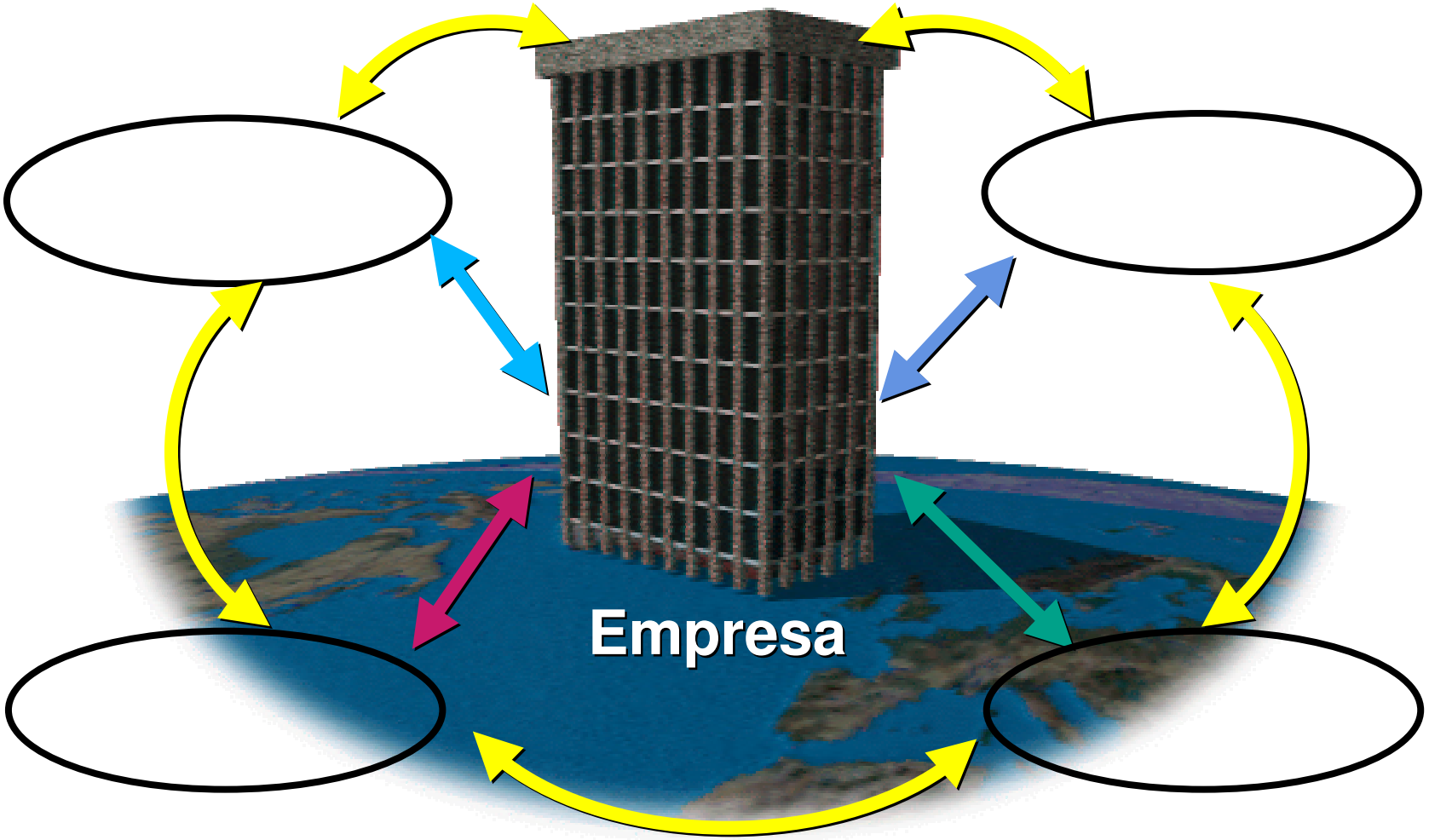
Chile : Sólo un 10% de las empresas denuncia ataques de hackers : La Tercera – Sept 2001



- Falta de Inversión
- Falta de profesionales especializados en protección de datos
- Habilidad de los piratas informáticos

FACTORES QUE INFLUYEN EN EL PROBLEMA

La Globalidad de los Negocios



Cambios en el e-Business

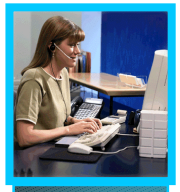
Base usuario Expandida

Nuevas Aplicaciones

Aumento de acceso a contenidos

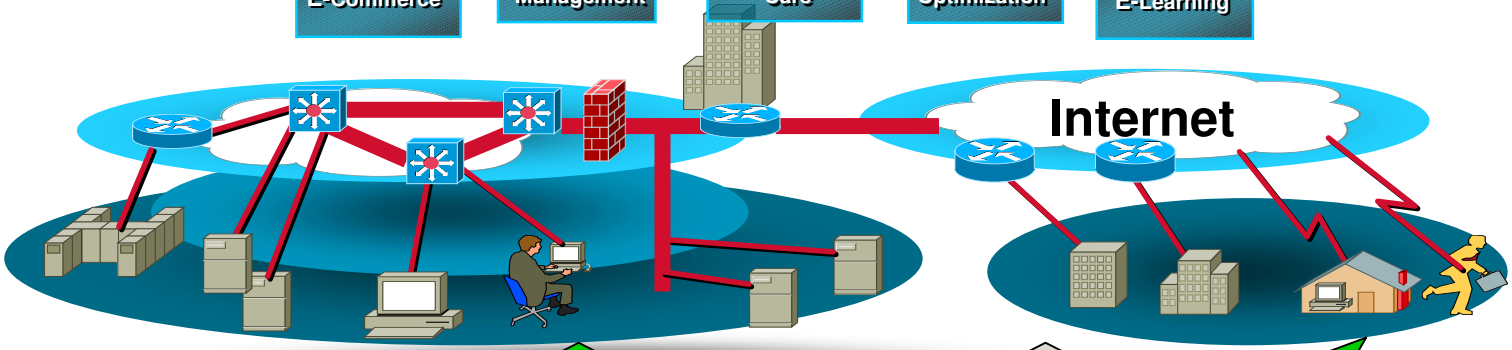

E-Commerce


Supply Chain Management


Customer Care


Workforce Optimization


E-Learning



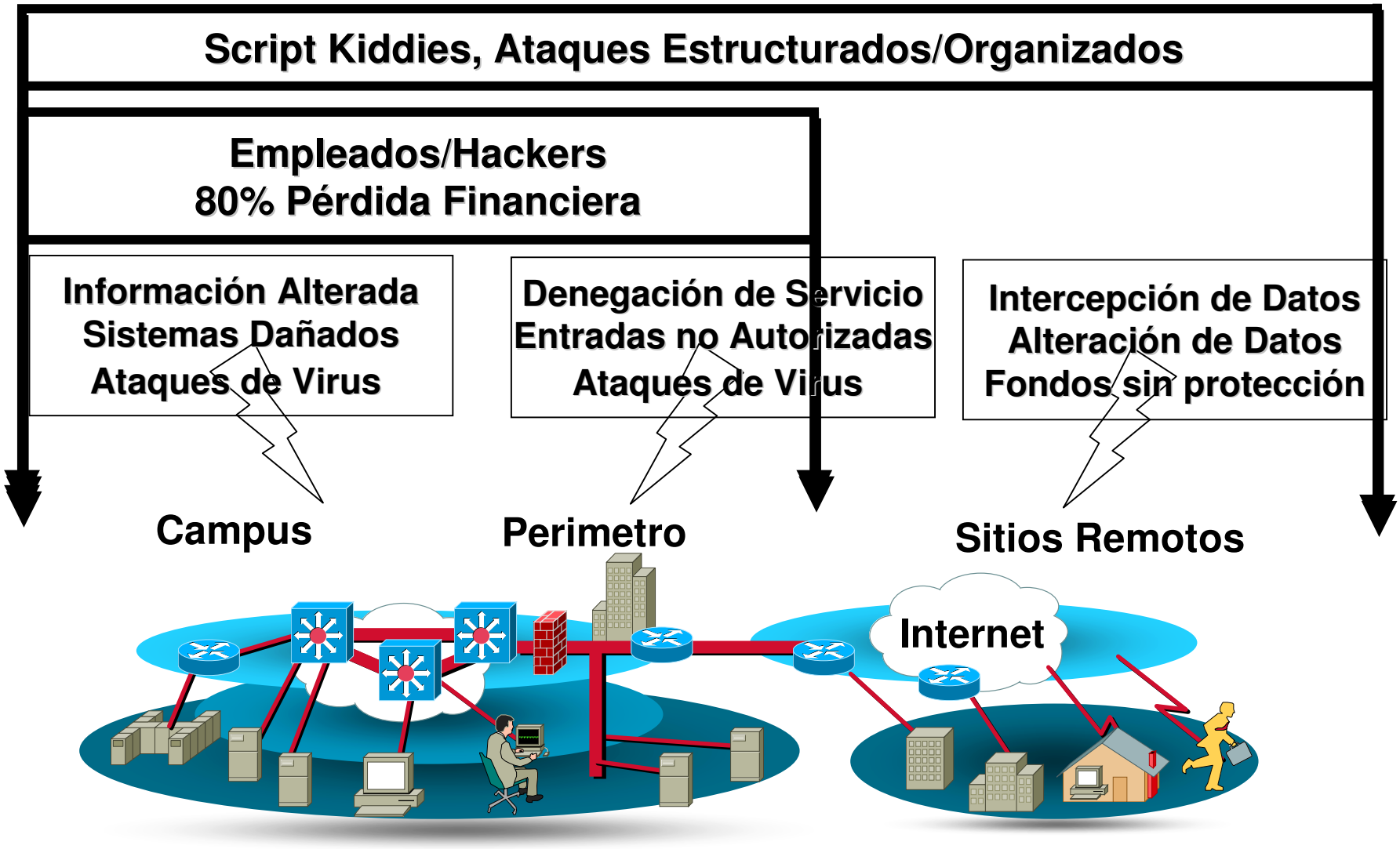
Escalibilidad

Administración

Seguridad

Disponibilidad

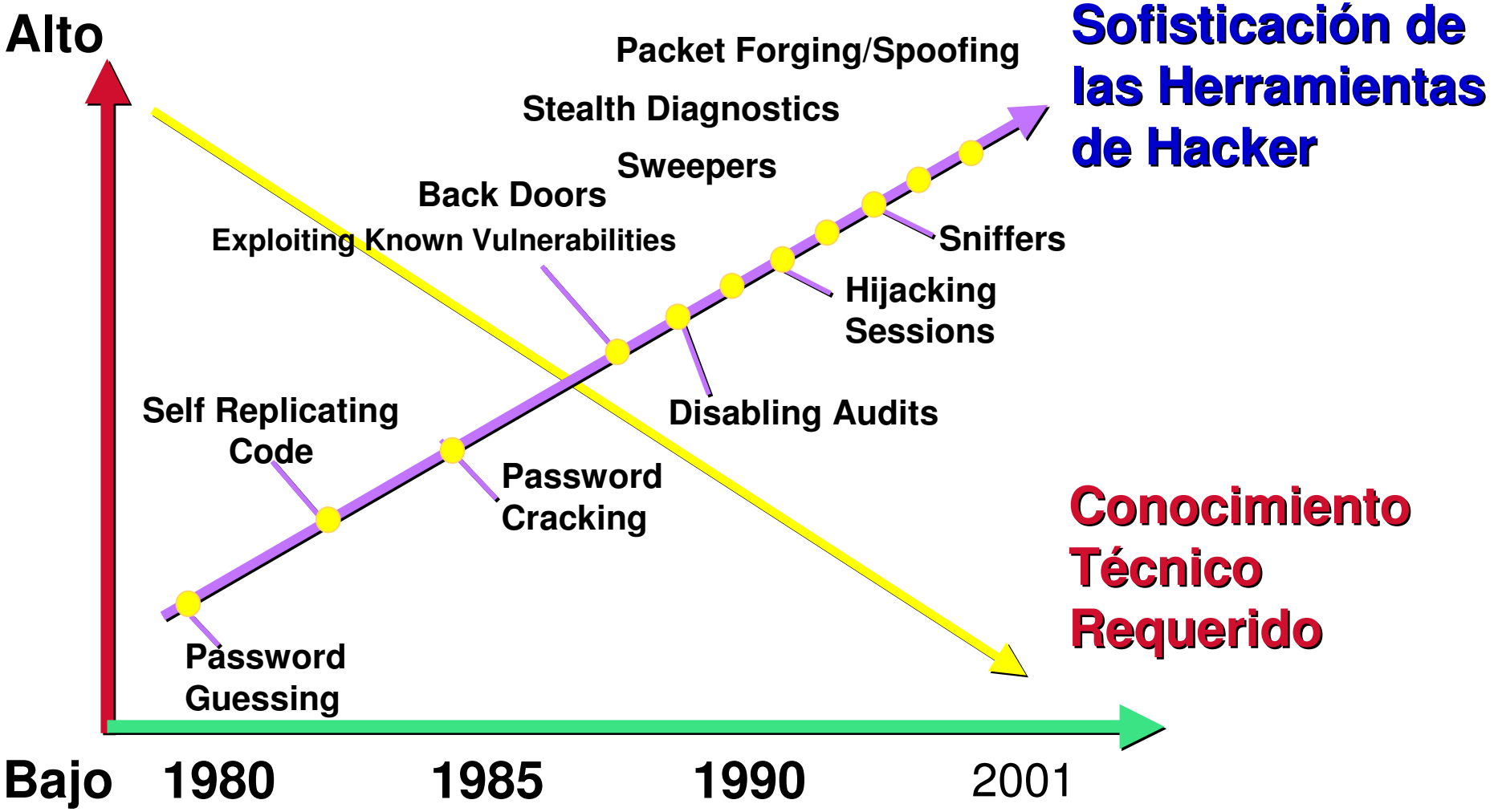
Cambios en la Seguridad



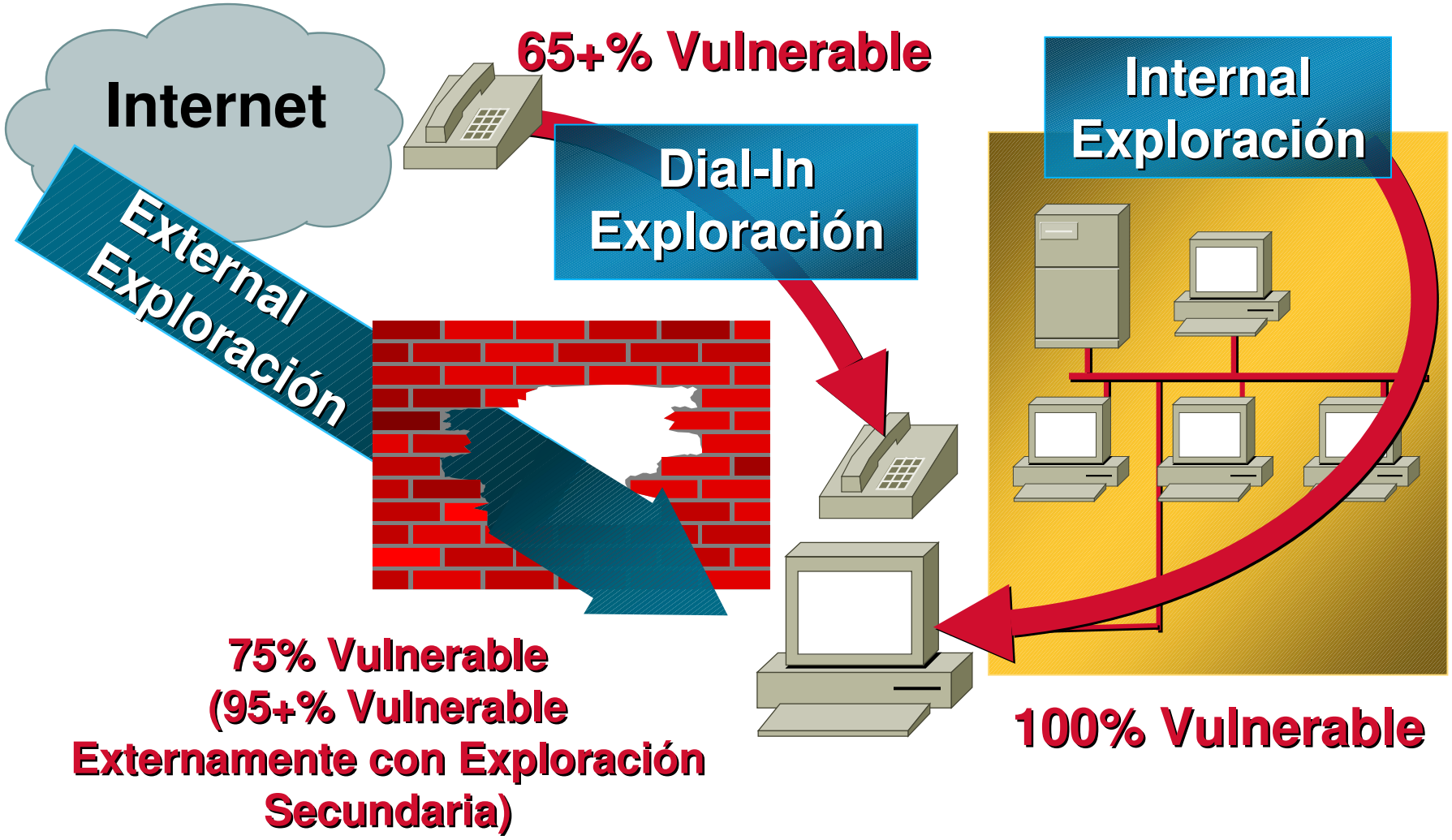
Seguridad : Cambios de Rol

- Requirida para e-business
- Haciendo negocios seguros en ambientes inseguros
- Estabilizando consistencia en políticas corporativas
- Administración y Control Centralizado
- Proceso continúo — requiere una defensa en profundidad

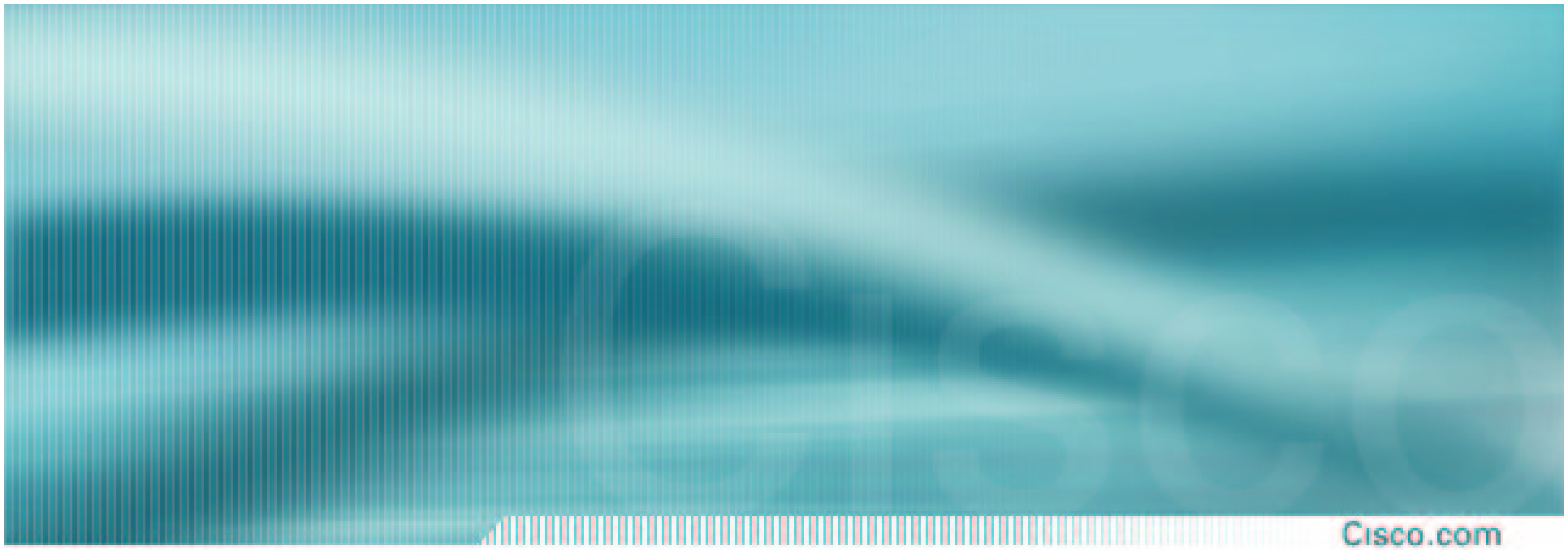
Tendencia en las Capacidades



Vulnerabilidades al Atacar Redes

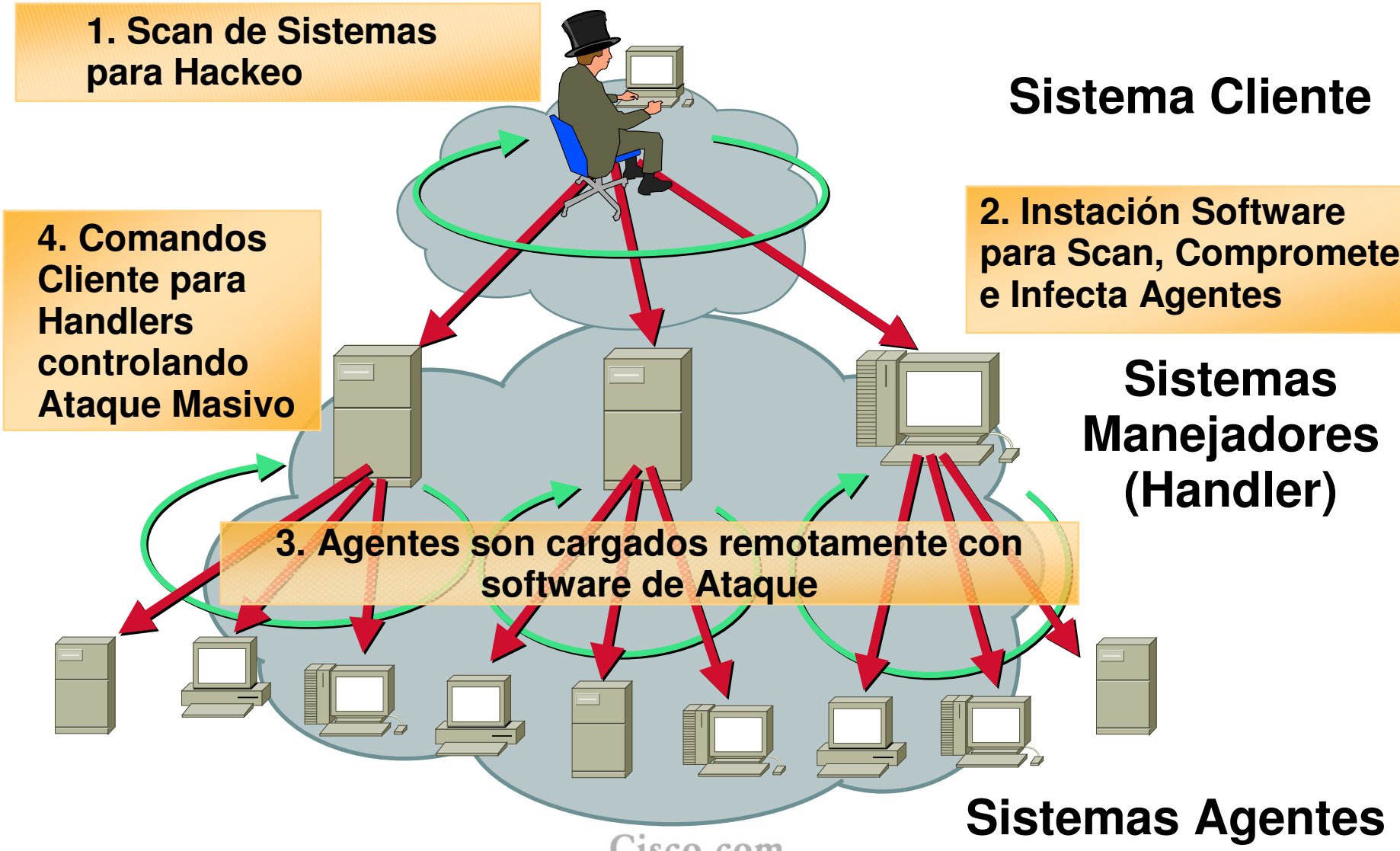


Source: Cisco Security Posture Assessments—All Figures Are Approximate

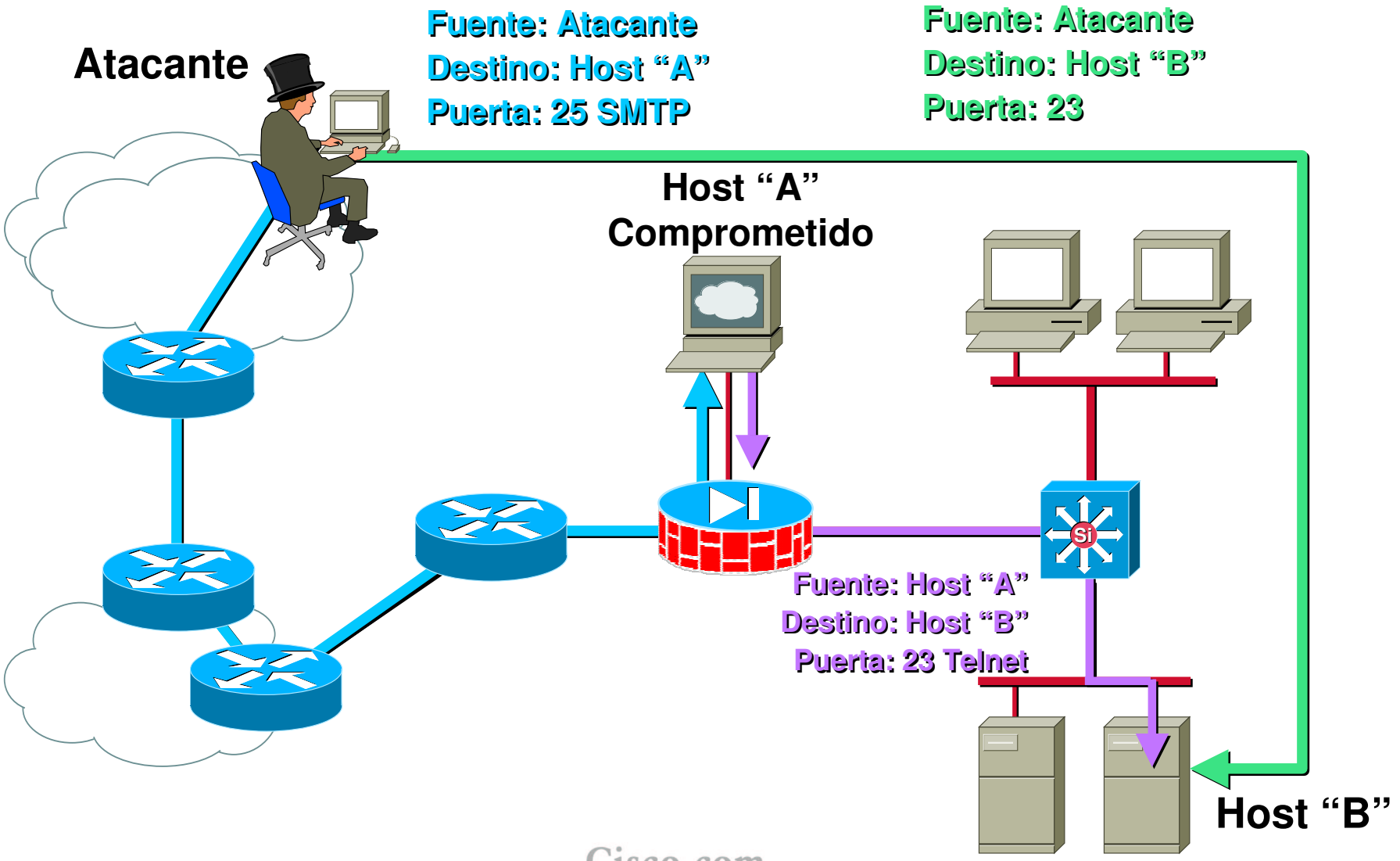


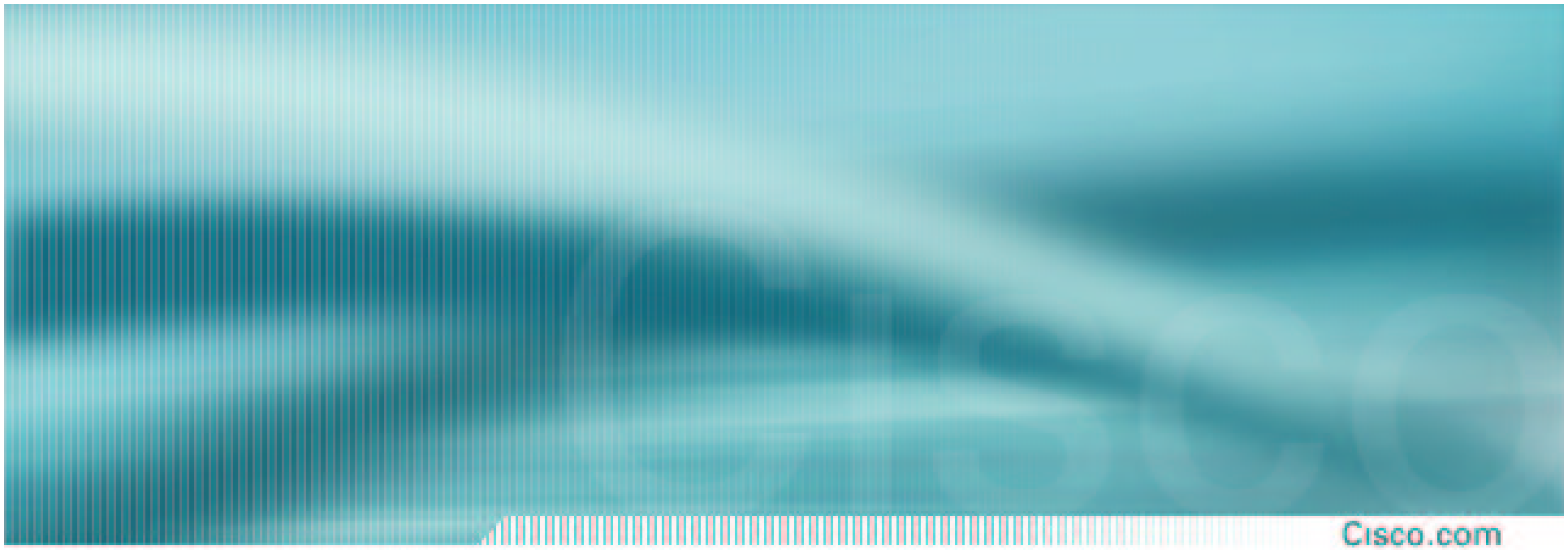
Hackers & Crackers

Distributed Denial of Service (DDoS) Cómo trabaja ?



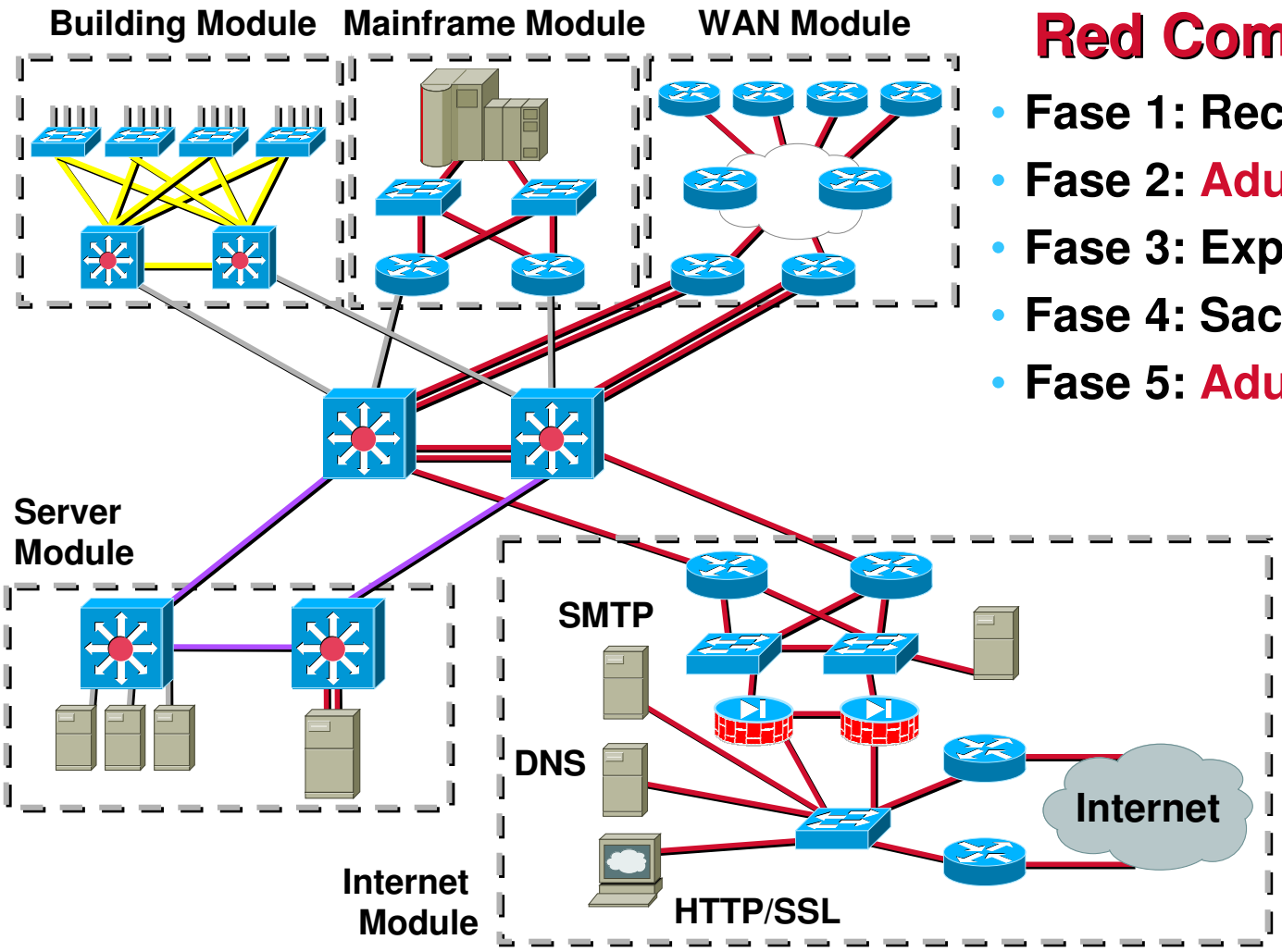
Ataque por Redirección de Puerta





Ataque

Invitemos a un Hacker!

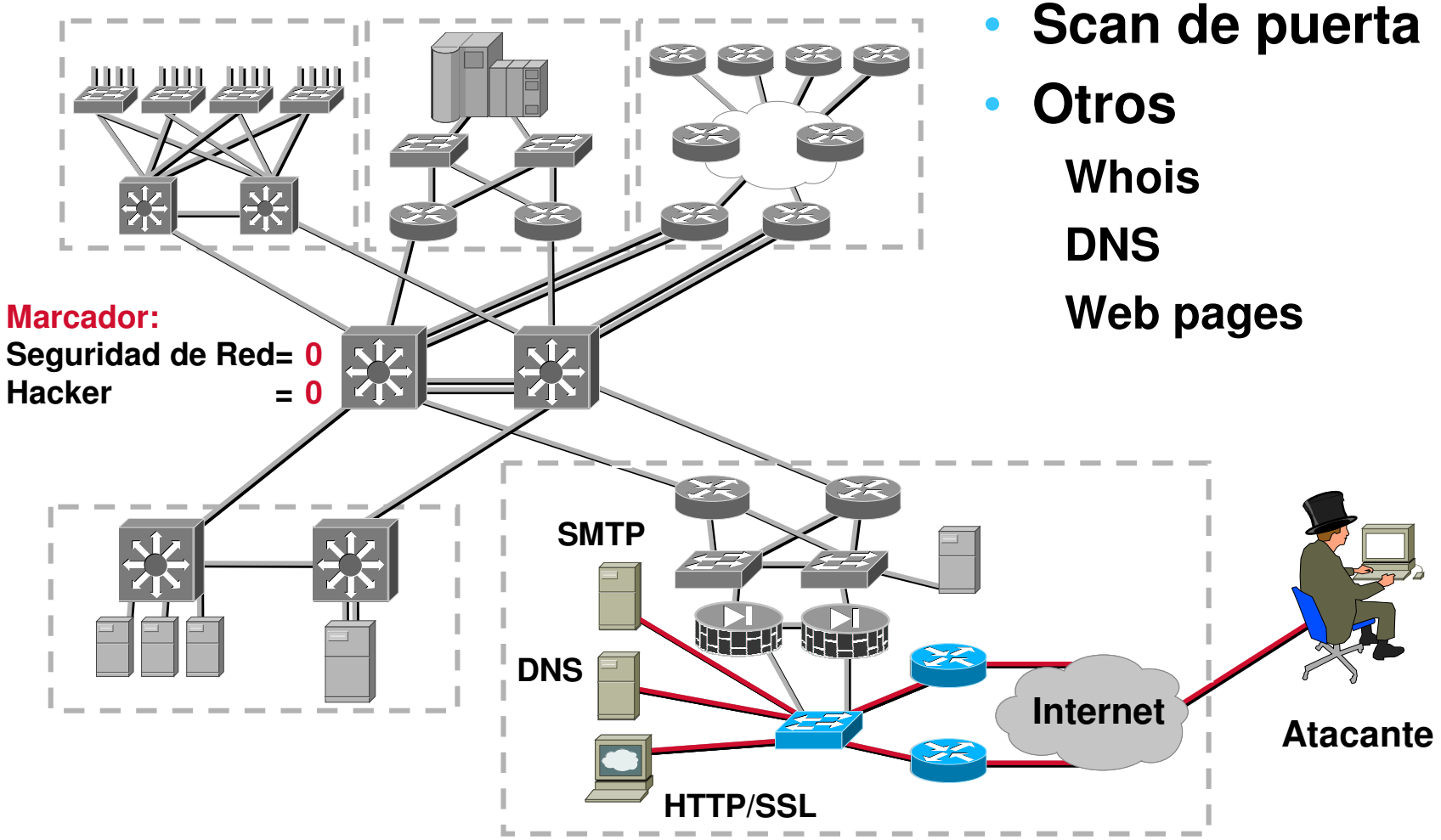


Red Comprometida

- Fase 1: Reconoc. Red
- Fase 2: Adueñarse de un sist.
- Fase 3: Explotac. Confianza
- Fase 4: Sacar Provecho
- Fase 5: Adueñarse de la Red

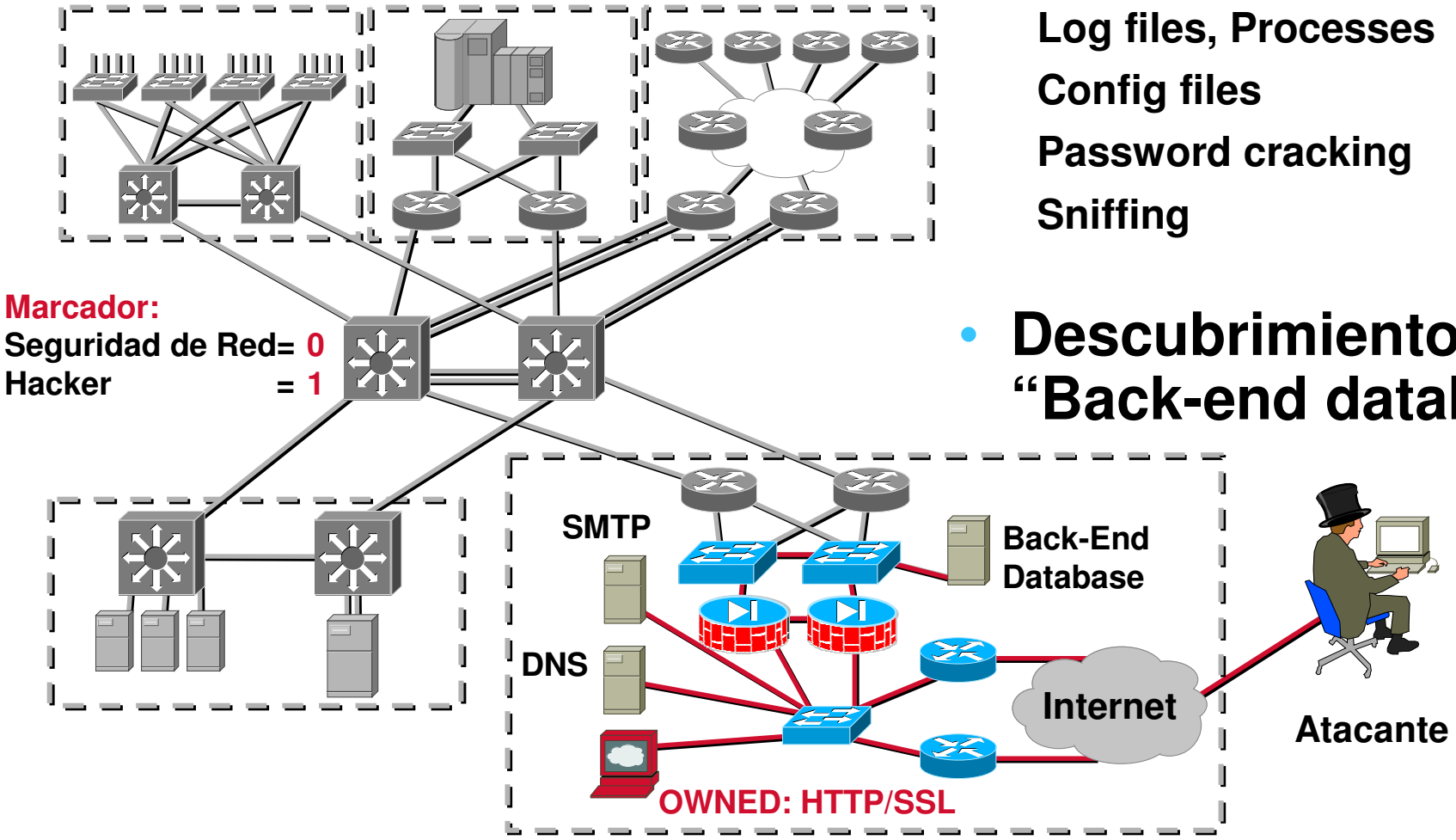
Reconocimiento de Red

- Ping barrido
- Scan de puerta
- Otros
  - Whois
  - DNS
  - Web pages



Explotación
Relaciones de Confianza

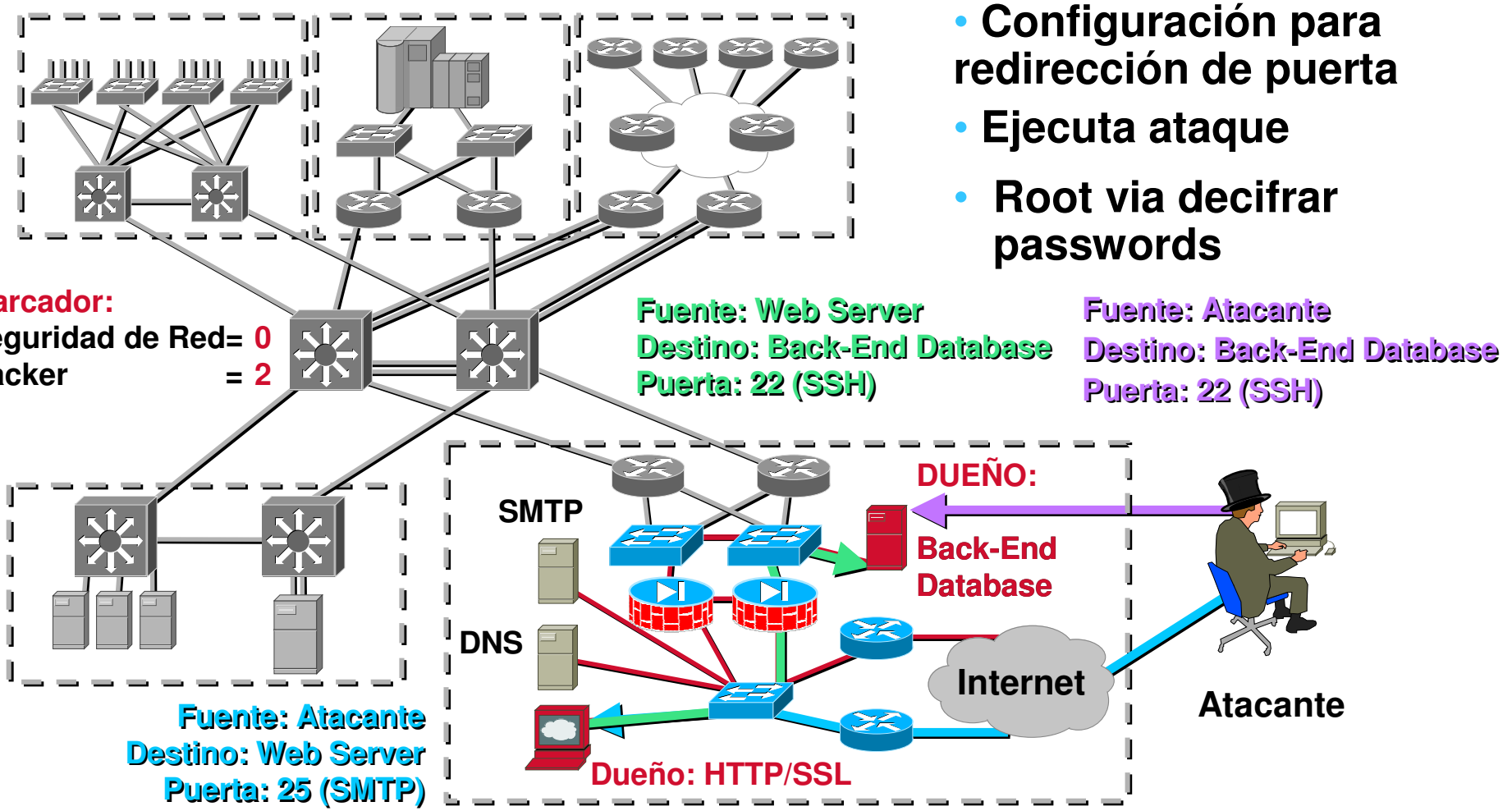
- **Más reconocimiento**
  - Log files, Processes
  - Config files
  - Password cracking
  - Sniffing



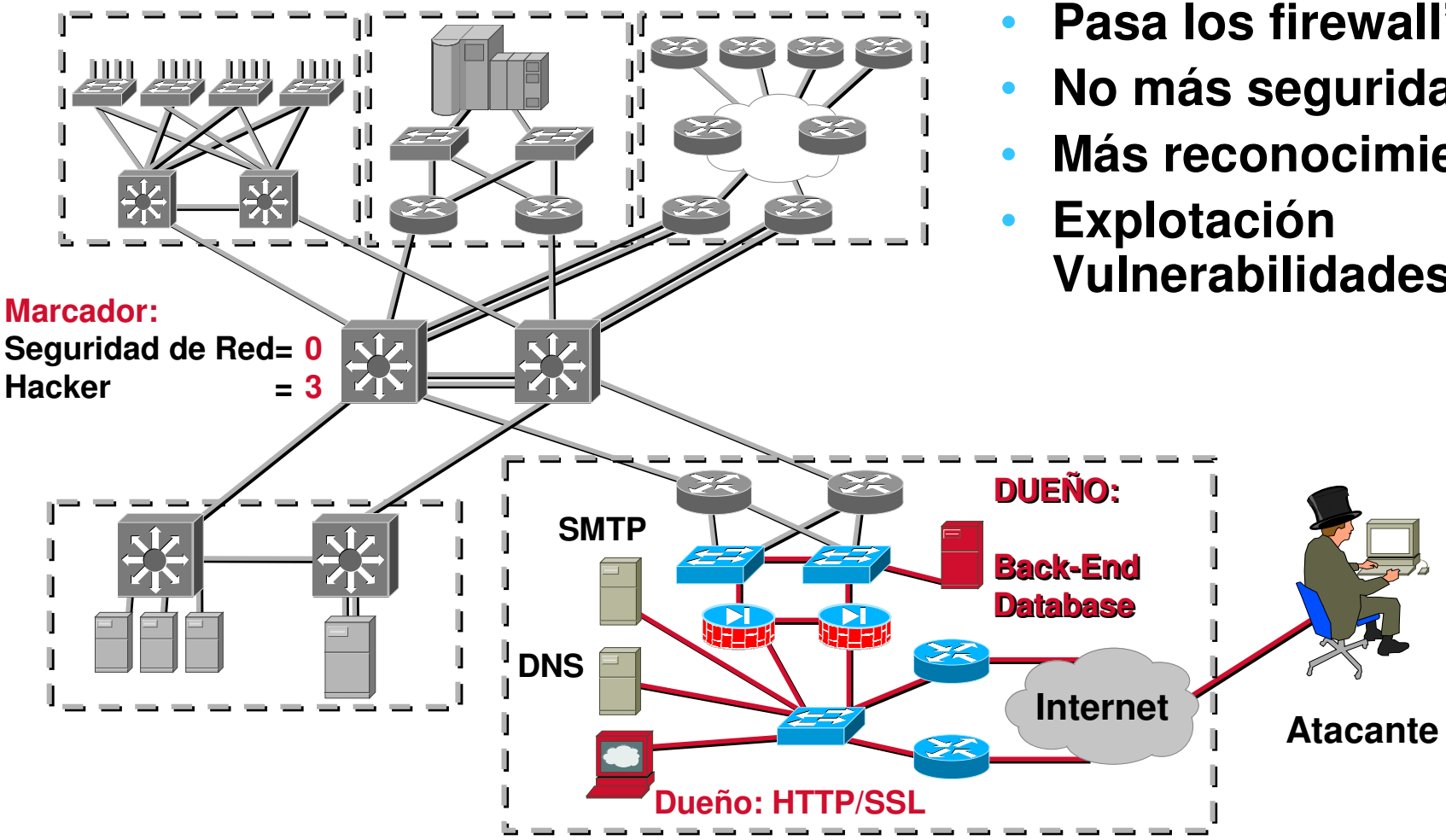
- **Descubrimiento de "Back-end database"**

Sacar Provecho!

- Configuración para redirección de puerta
- Ejecuta ataque
- Root via decifrar passwords

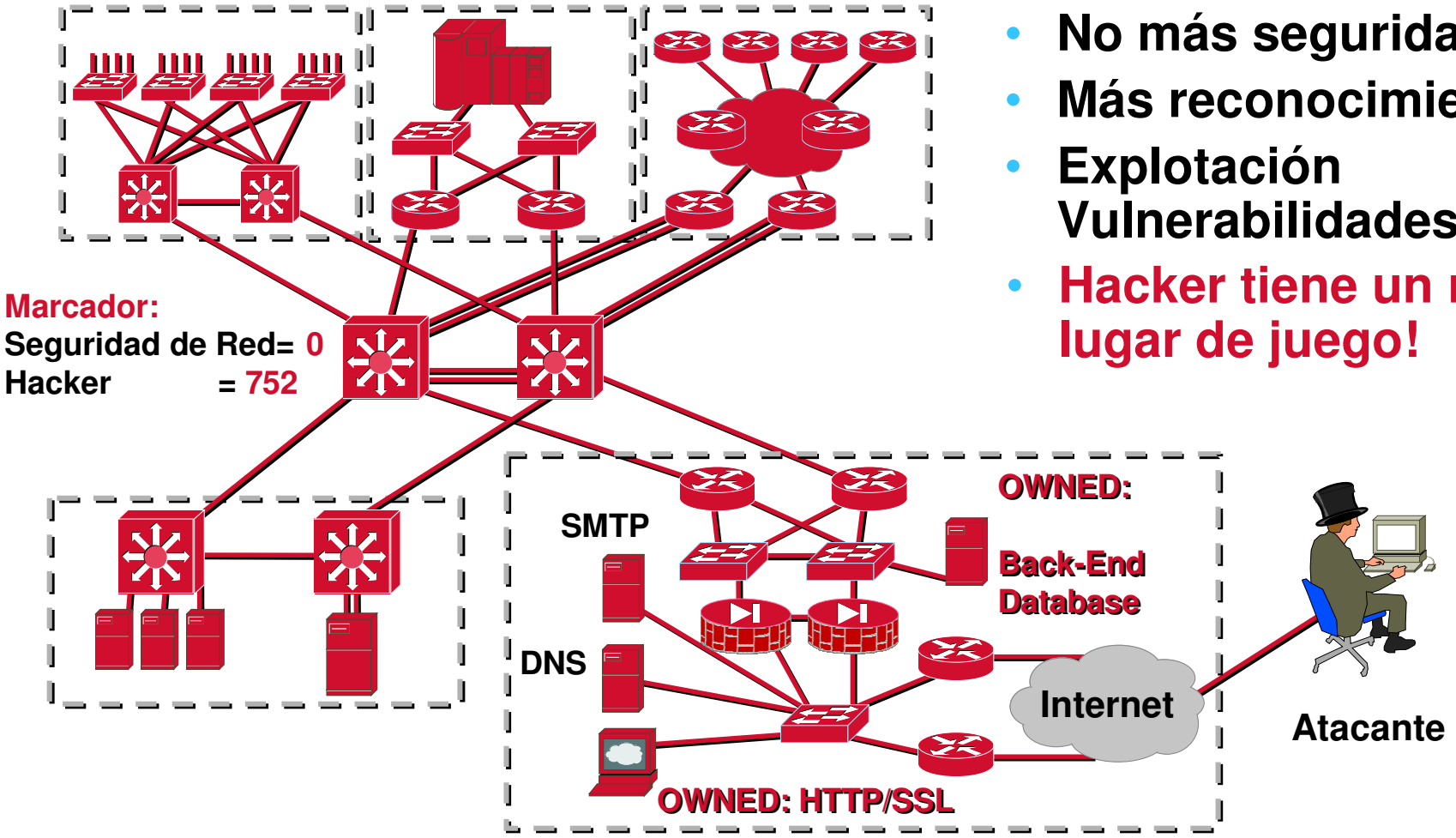


Dueño de la Red



- Pasa los firewall's
- No más seguridad
- Más reconocimiento
- Explotación Vulnerabilidades

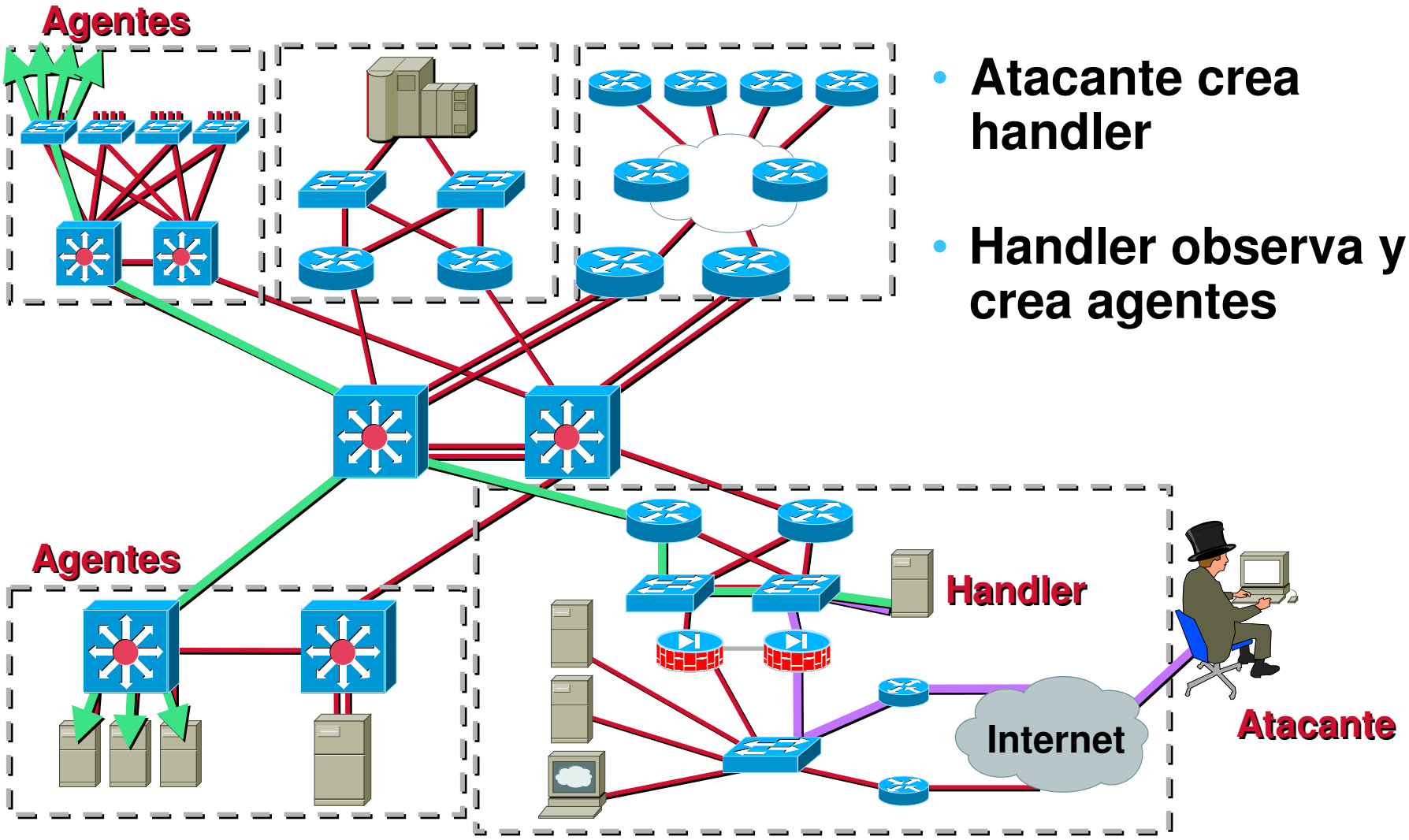
Dueño Total de la Red



- Pasa los firewall's
- No más seguridad
- Más reconocimiento
- Explotación Vulnerabilidades
- Hacker tiene un nuevo lugar de juego!

Nuestra Red ...

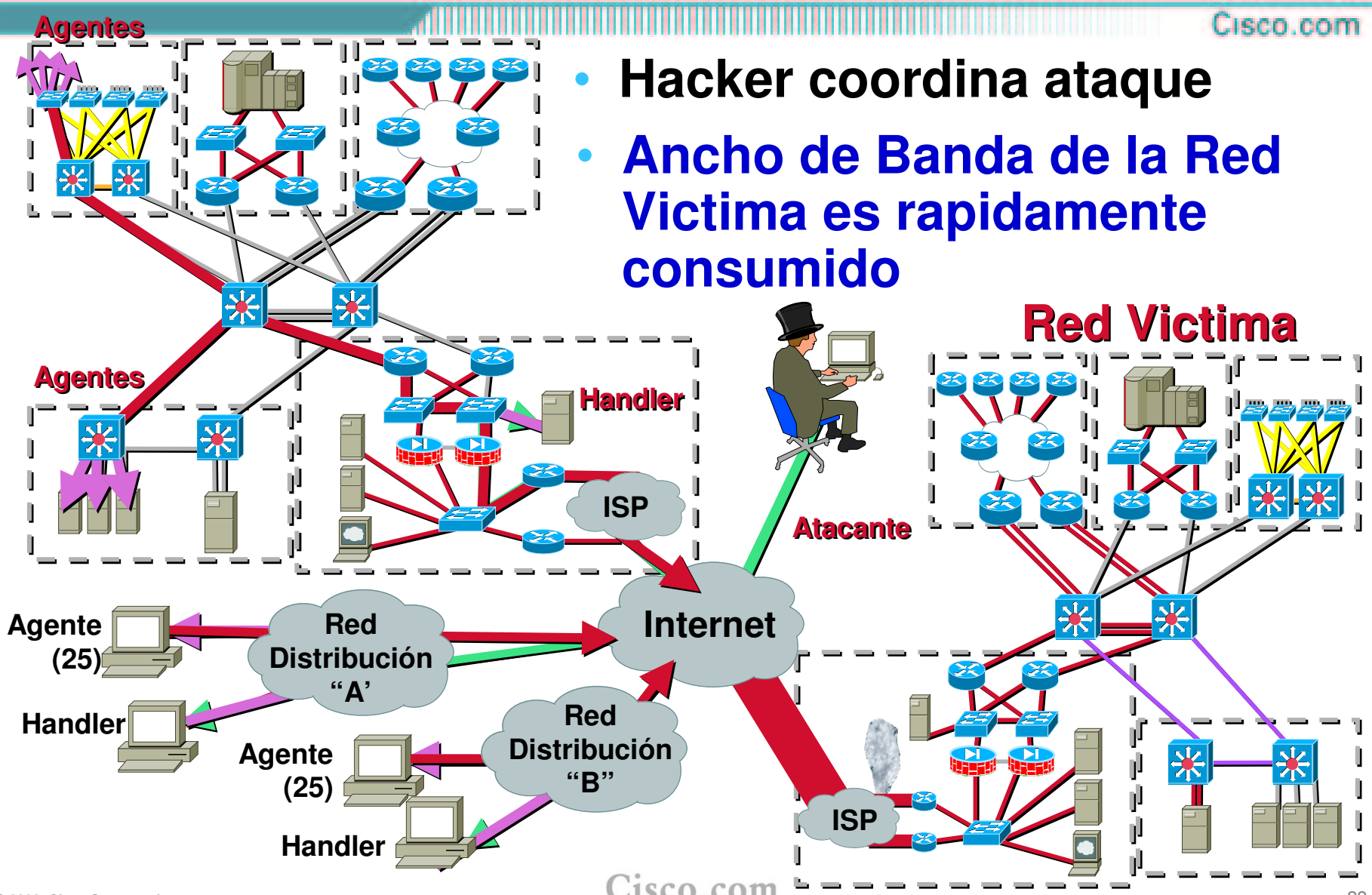
Configurando una Distribución de Red



- Atacante crea handler
- Handler observa y crea agentes

Ataque !!!

- Hacker coordina ataque
- Ancho de Banda de la Red Victima es rapidamente consumido



Ataque – Revisión

- **Red comprometida fue completamente accesada**

  Firewall actuaron según configuración

- **DDoS fue completamente exitoso**

  Ancho de Banda disponible para Internet fue consumido

  Medidas de protección DDoS en routers y firewalls no fueron considerados

Distributed Denial of Service (DDoS)

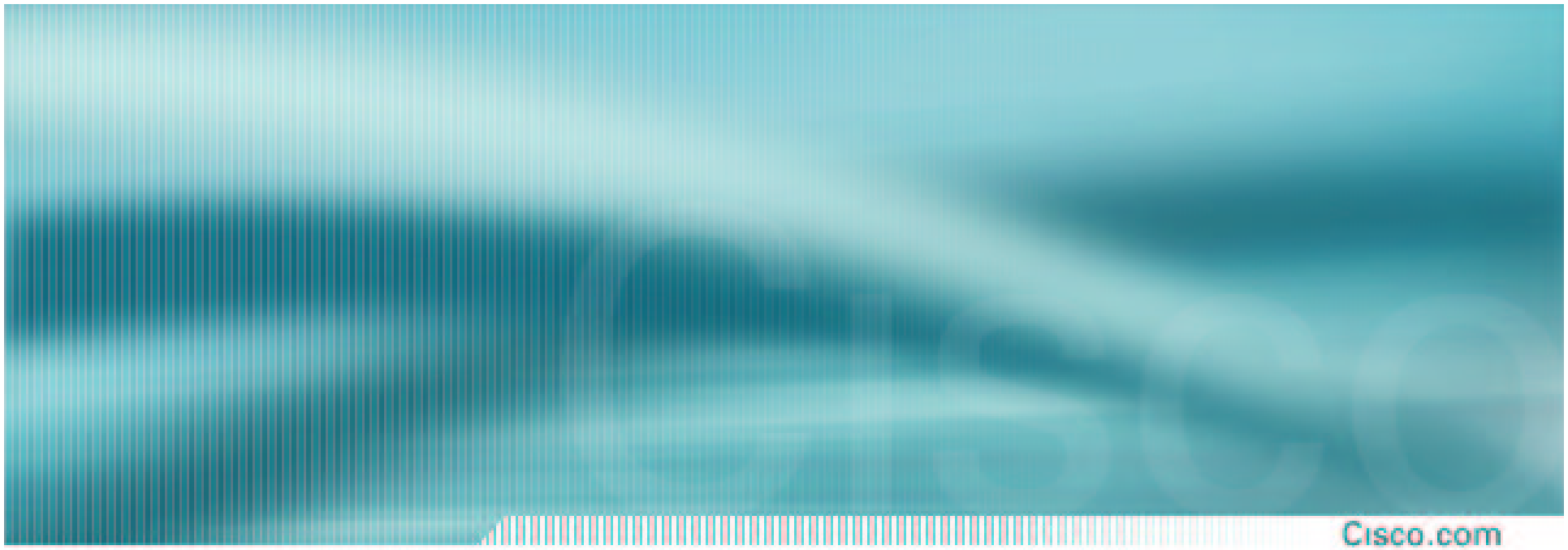
YAHOO!

amazon.com

CNN.com

ebay

E*TRADE



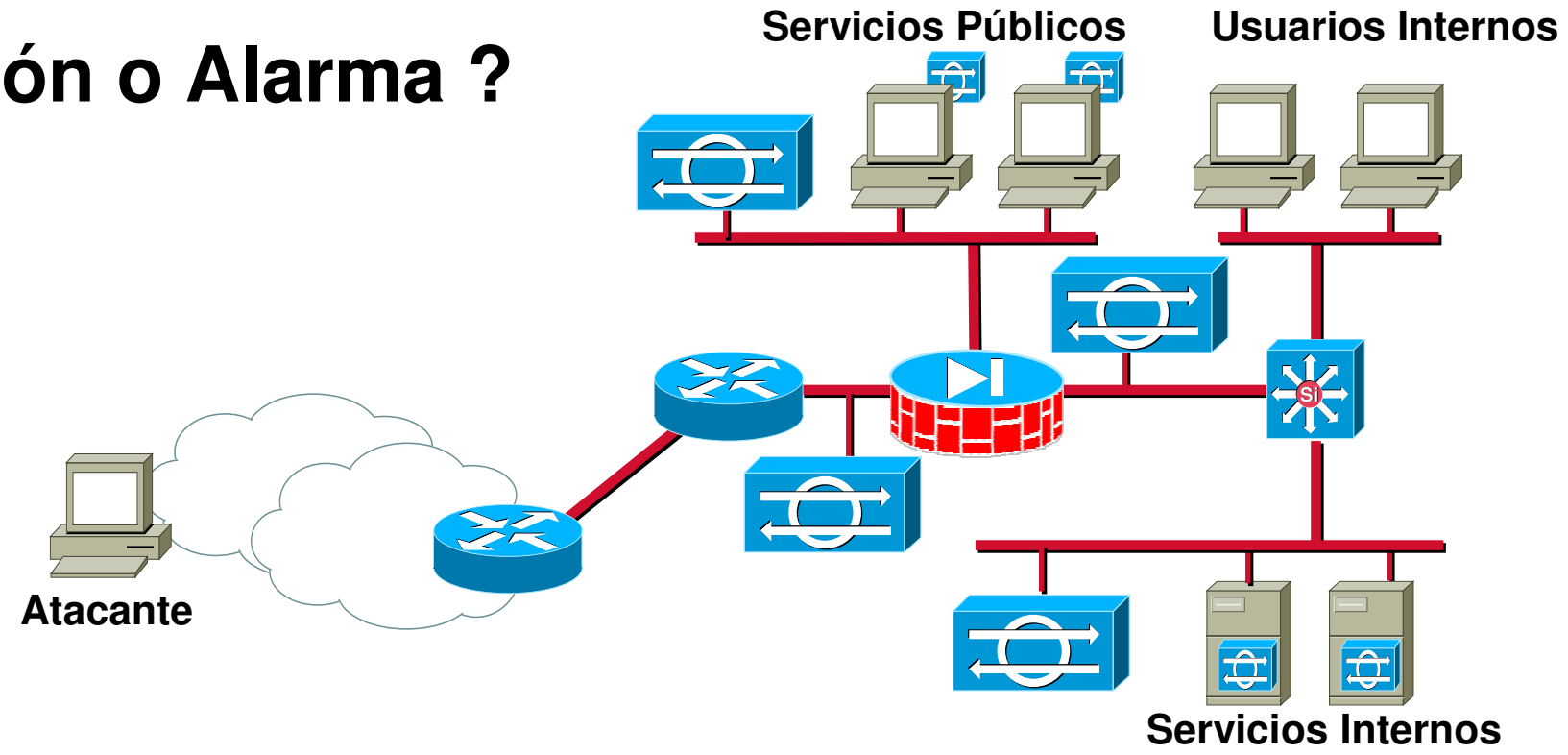
Técnicas en Seguridad

Sistemas para Detección de Intrusos (IDS)

- **Host IDS y Network IDS**

  Ambos tiene su lugar

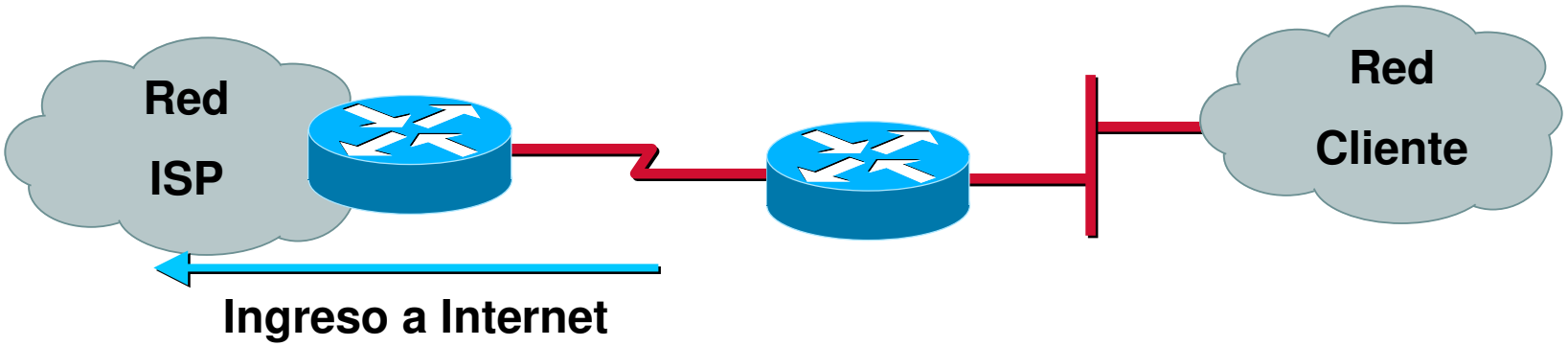
- **Acción o Alarma ?**



Commited Access Rate (CAR)
Velocidad de Acceso Comprometida

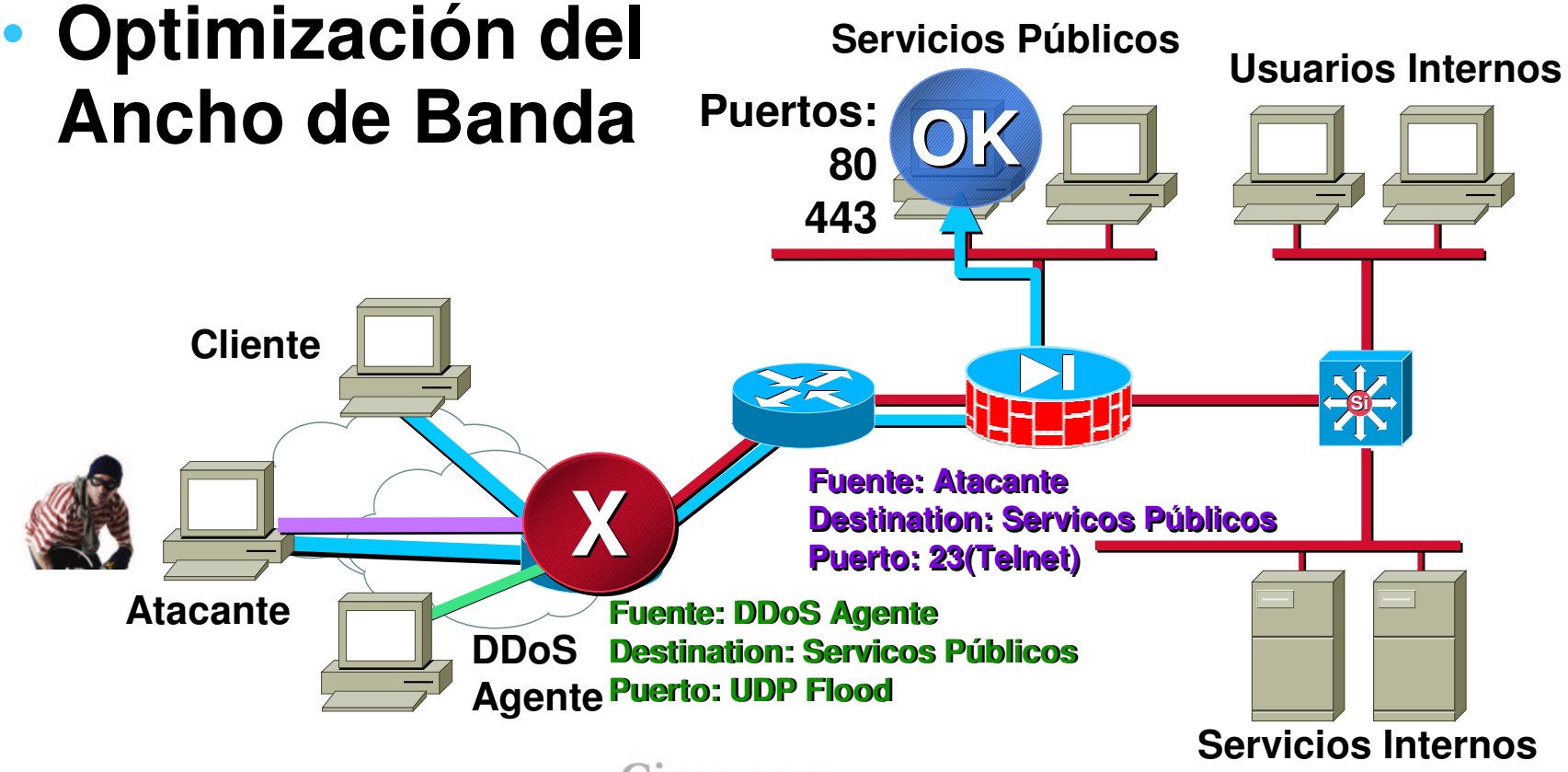
Limite en ping de salida a 256 Kbps

```
interface xy
      rate-limit output access-group 102 256000 8000 8000
            conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```



Filtraje en el Proveedor de Servicios (ISP)

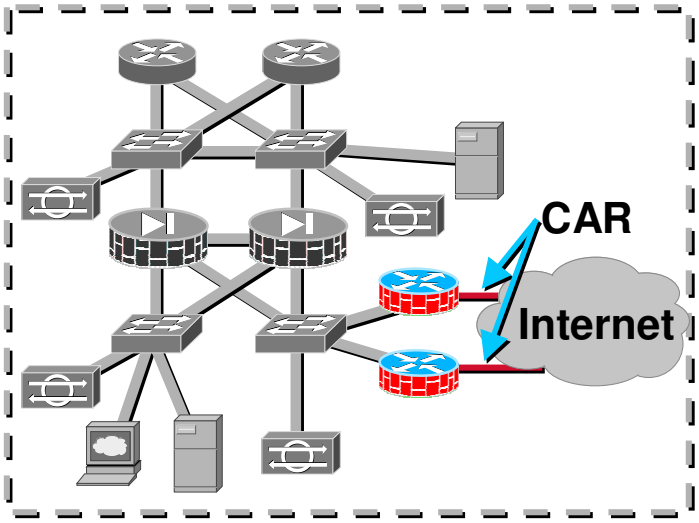
- DDoS mitigación
- Optimización del Ancho de Banda



Acceso a Router
Access Control List (ACL)

Filtros Específicos para Servicos de Salida

Source	Destination	Protocol	Action
Internal	Any	Any	Permit
Mail Server	Outside	SMTP	Permit
DNS	Outside	DNS	Permit

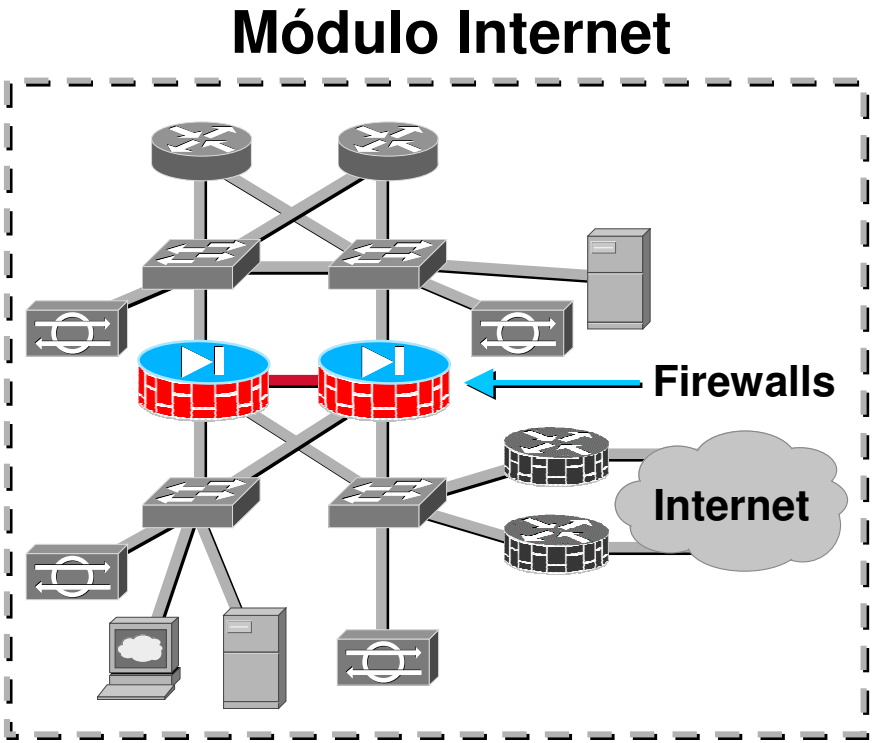


Módulo Internet

Filtros Específicos para todos los servicios

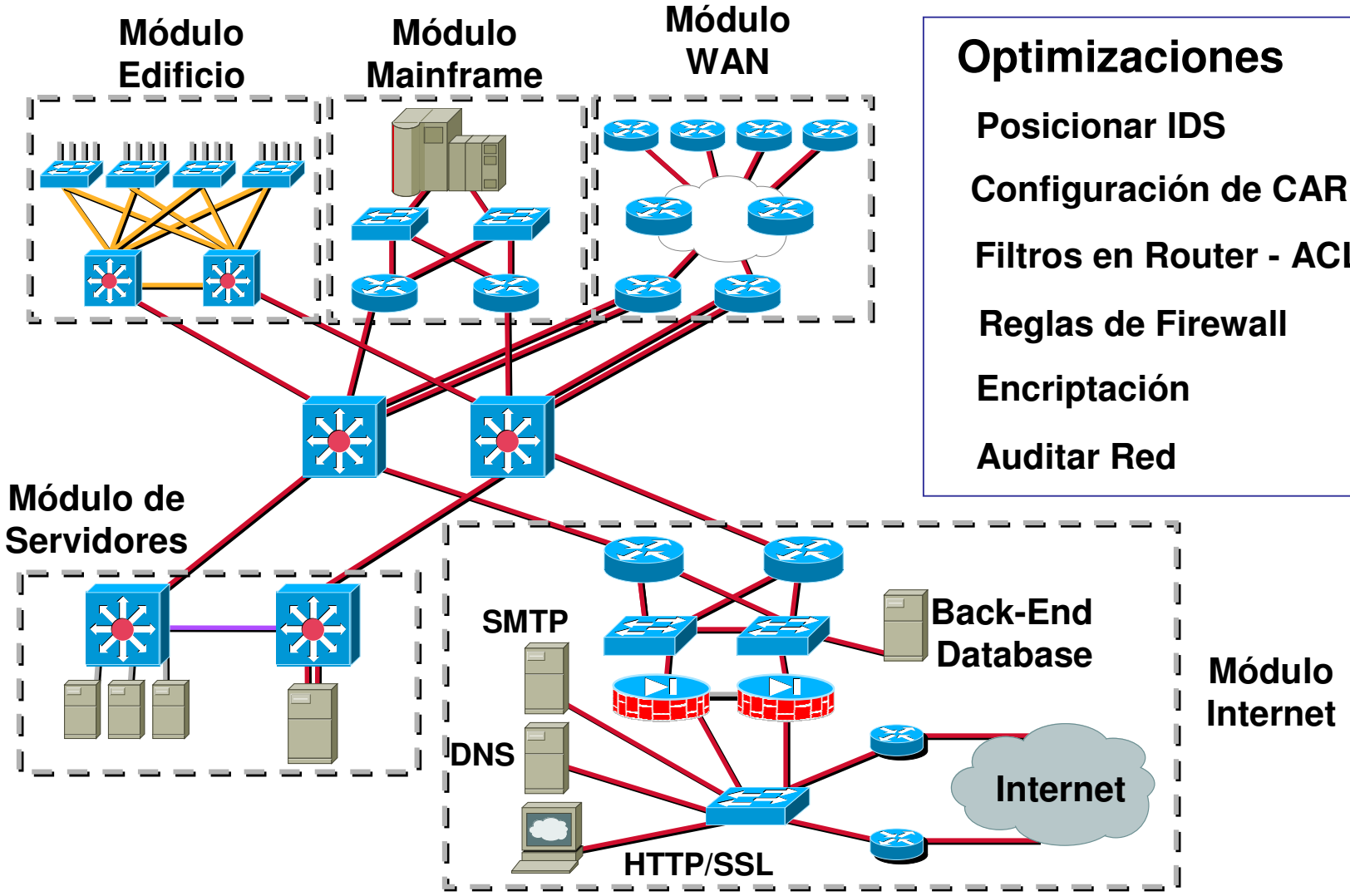
Source	Destination	Protocol	Action
Outside	Mail Server	SMTP	Permit
Outside	Web Server	HTTP	Permit
Outside	DNS Server	DNS	Permit
Outside	Web Server	SSL	Permit

Reglas de Firewall´s



Source	Destination	Protocol	Action
Internal	Any	Any	Permit
Web Server	Back-End Database	SQL	Permit
Pub. SMTP	Int. SMTP and Outside	SMTP	Permit
DNS	Outside	DNS	Permit
Outside	Mail Server	SMTP	Permit
Outside	Web Server	HTTP	Permit
Outside	DNS Server	DNS	Permit
Outside	Web Server	SSL	Permit

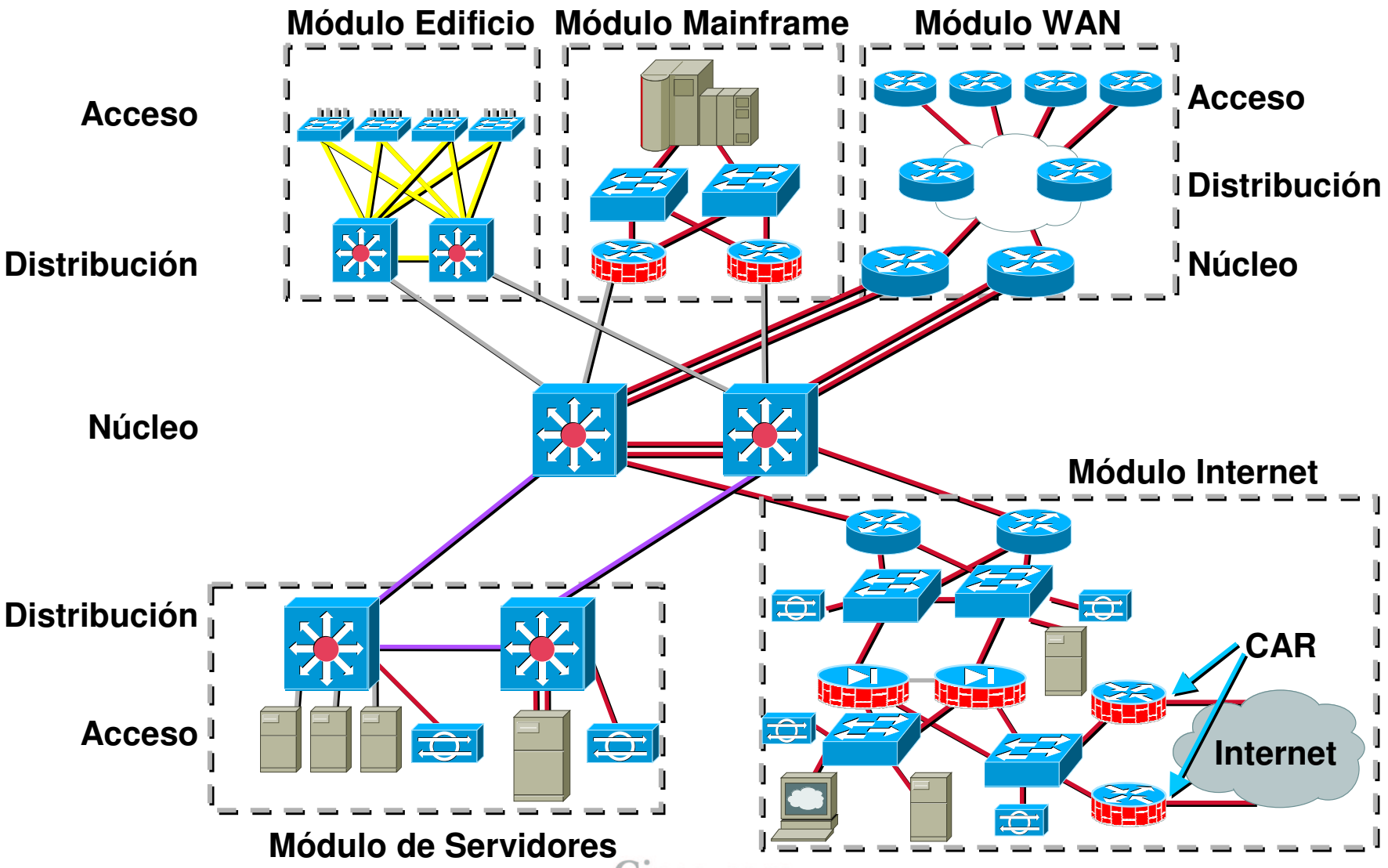
Optimización del Diseño



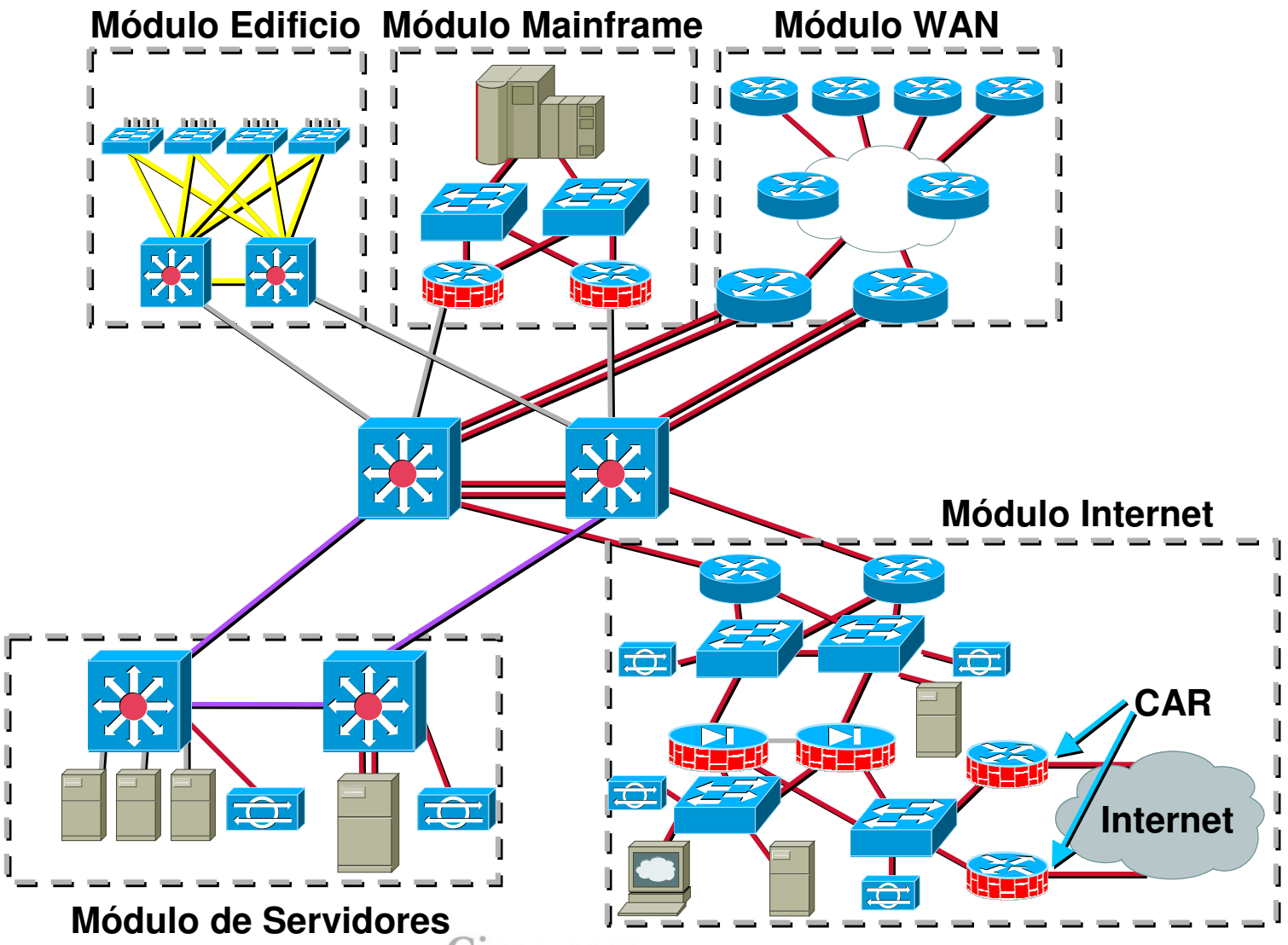
Optimizaciones

- Posicionar IDS
- Configuración de CAR
- Filtros en Router - ACL
- Reglas de Firewall
- Encriptación
- Auditar Red

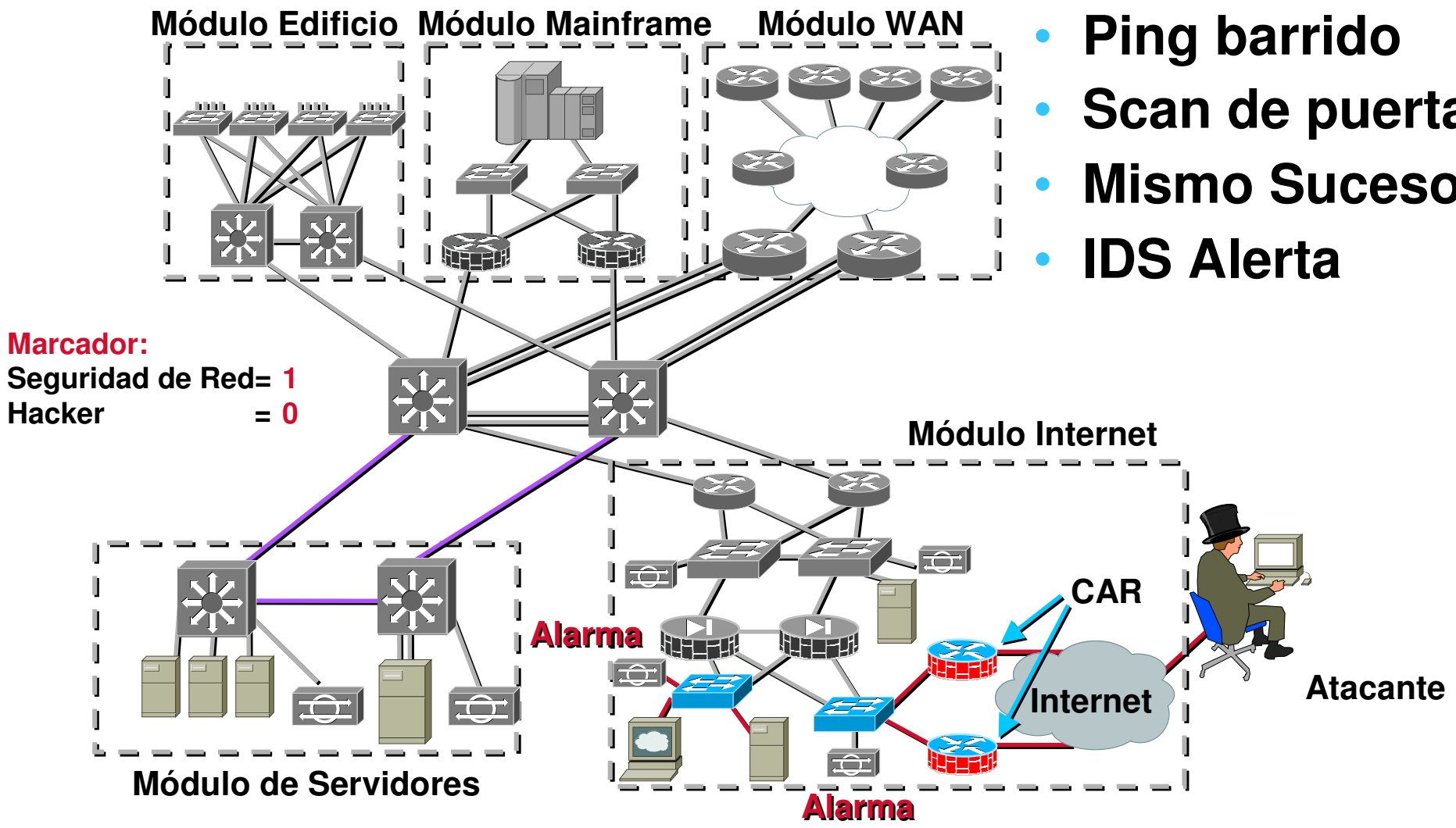
Diseño de Seguridad
Defensa en Profundidad



Invitemos a nuestro amigo Hacker nuevamente

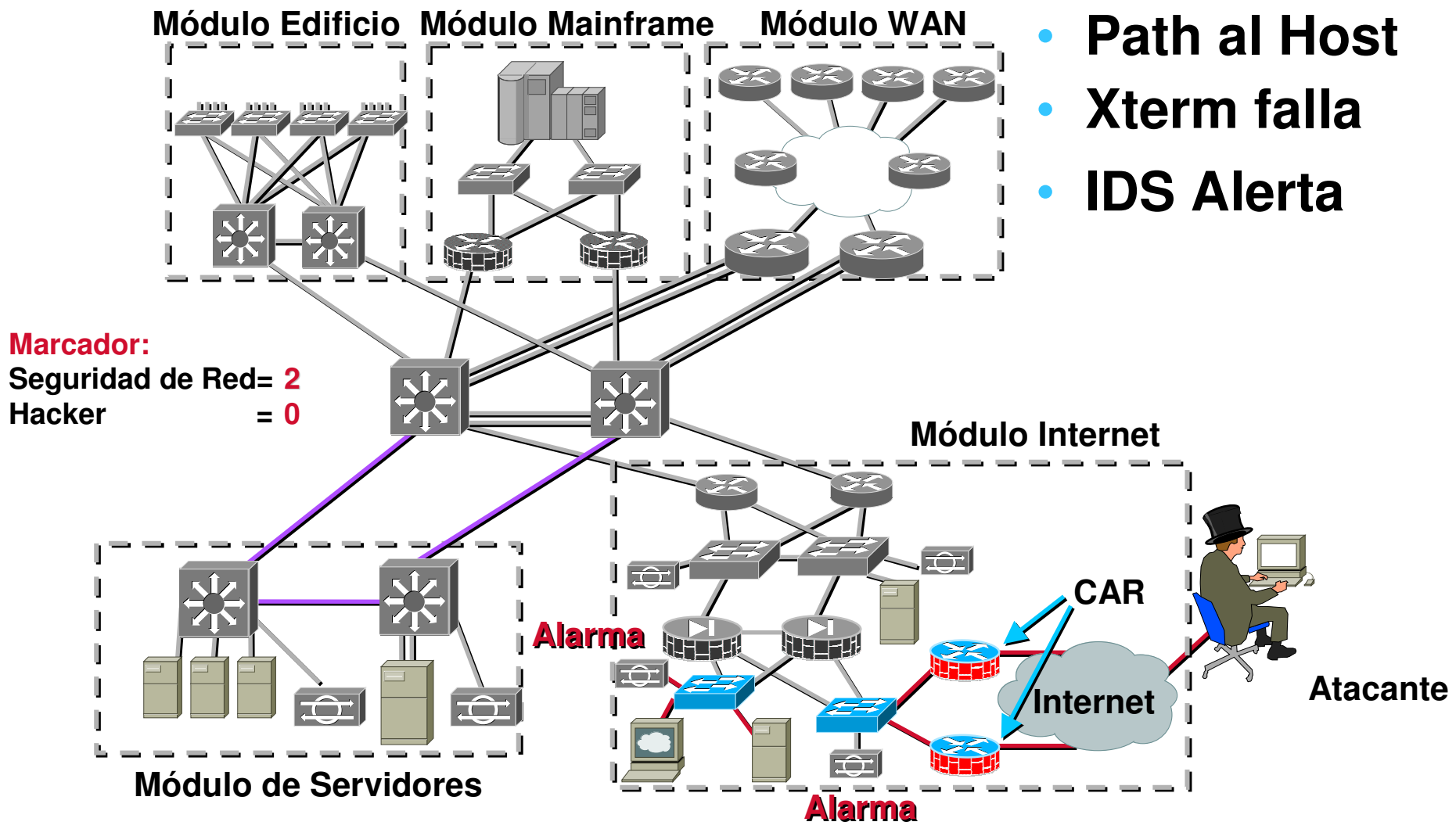


Reconocimiento de Red



- Ping barrido
- Scan de puerta
- Mismo Suceso
- IDS Alerta

Procurando Aduenãrse de la Red

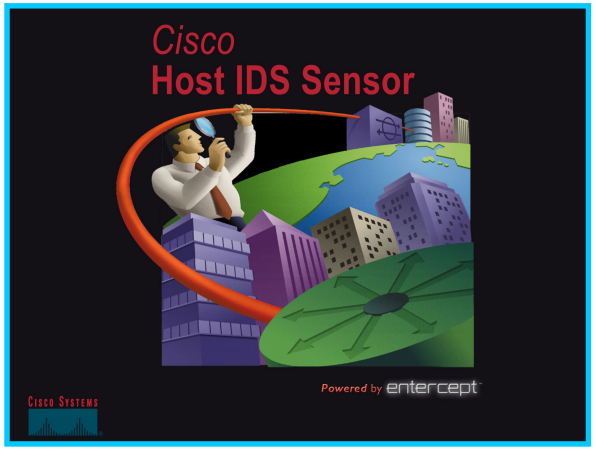


- Path al Host
- Xterm falla
- IDS Alerta

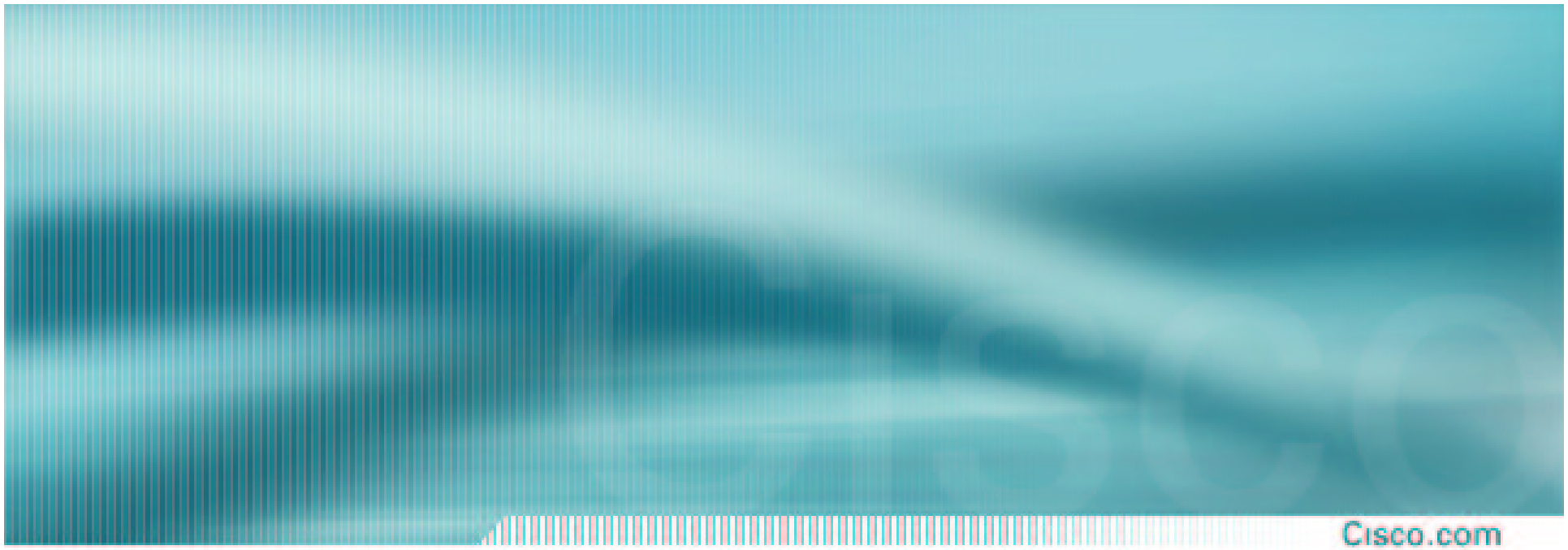
Ataque - Resumen

- **Red comprometida no pudo ser accesada**

  IDS – Alarmaron actividad



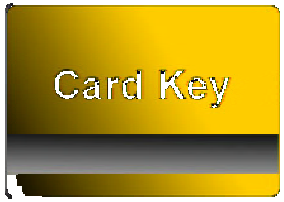
- **Sistemas corregidos adecuadamente**

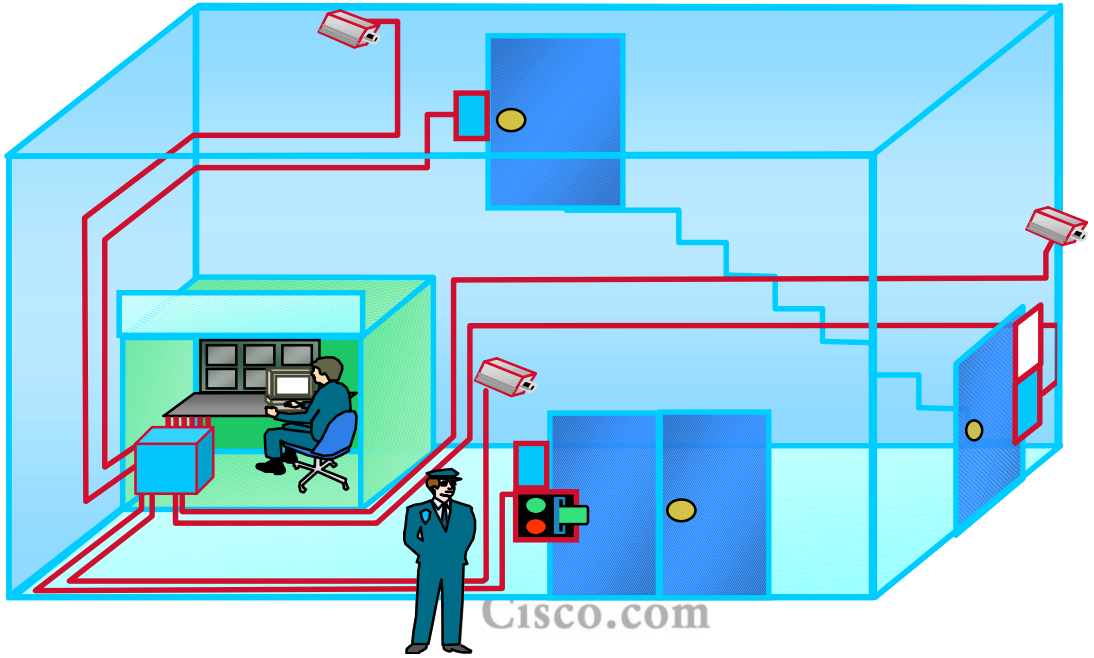


Arquitectura de Seguridad

Componetes de Seguridad del Mundo Físico

Cisco.com

Identidad	Seguridad Perimetral	Conectividad Segura	Monitoreo Seguridad	Admin. de Seguridad
				
	Chapas Tradicionales	Transporte Blindado	Guardias y Cámaras de Seguridad	Oficina de Seguridad



Componentes de Seguridad en la Red

1. Corporate Security Policy

2. Identidad

Autenticación
Certif. Digitales

3. Seguridad Perimetral

ACLs
Firewalls

4. Conectiv Segura

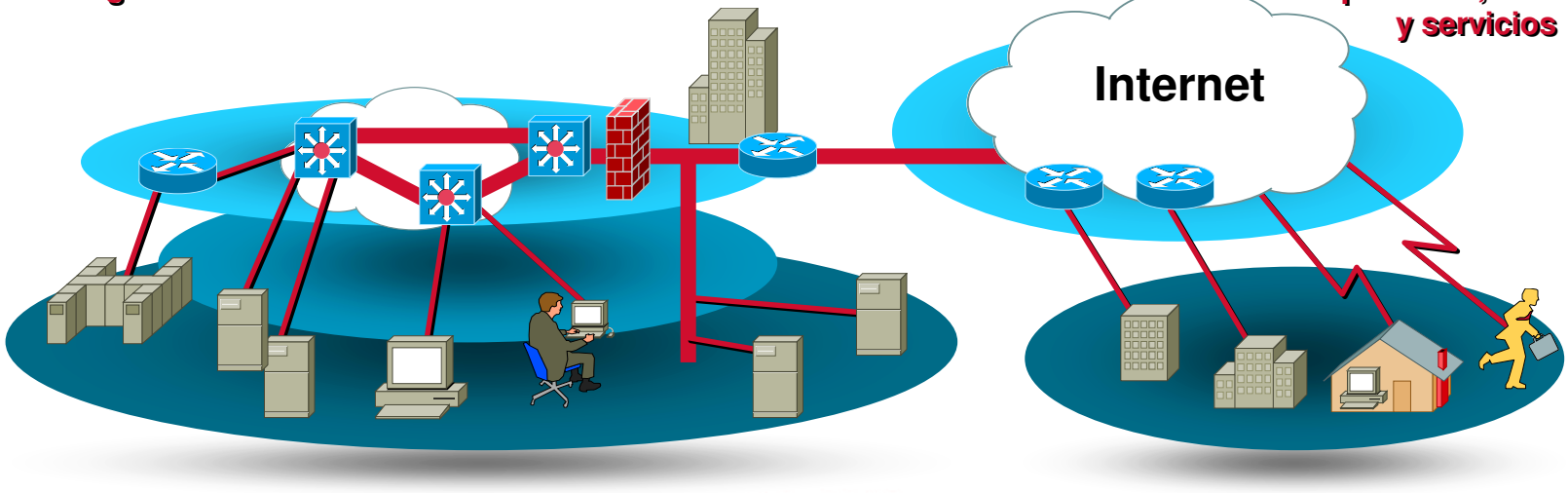
Tuneles VPN
Encriptación

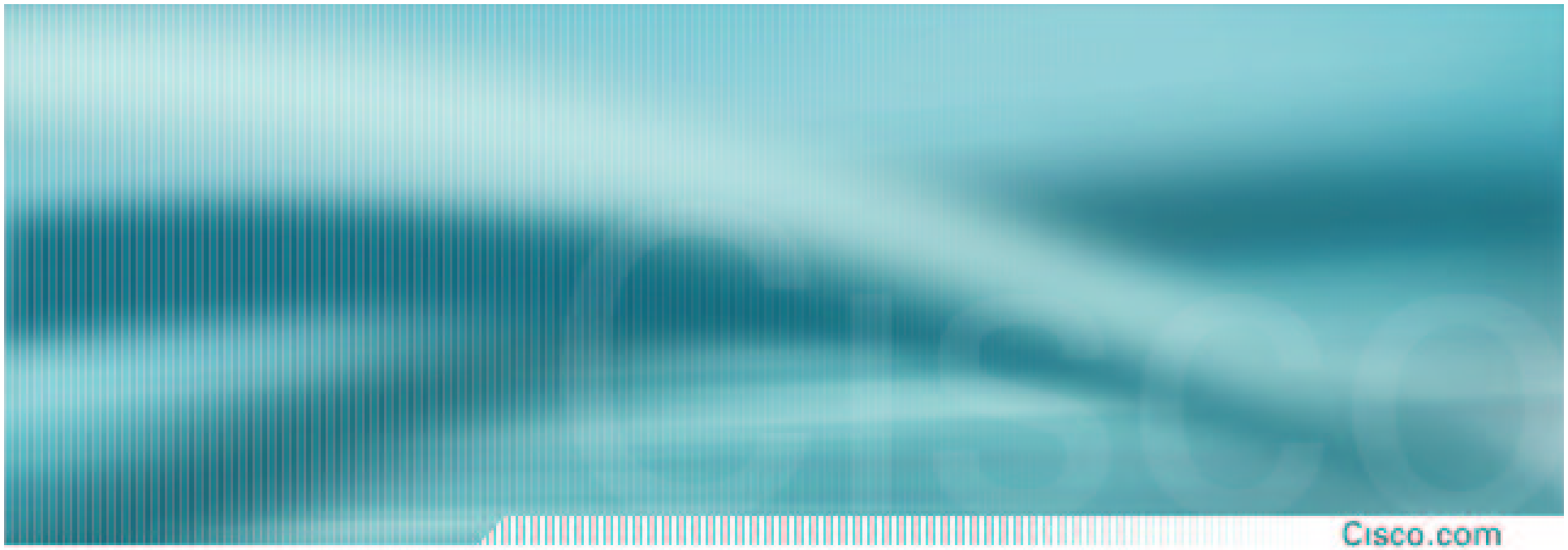
5. Monitoreo Seguridad

Detección Intrusos
Scanning

6. Admin. Seguridad

Admin. De Politicas, dispositivos, directorios y servicios



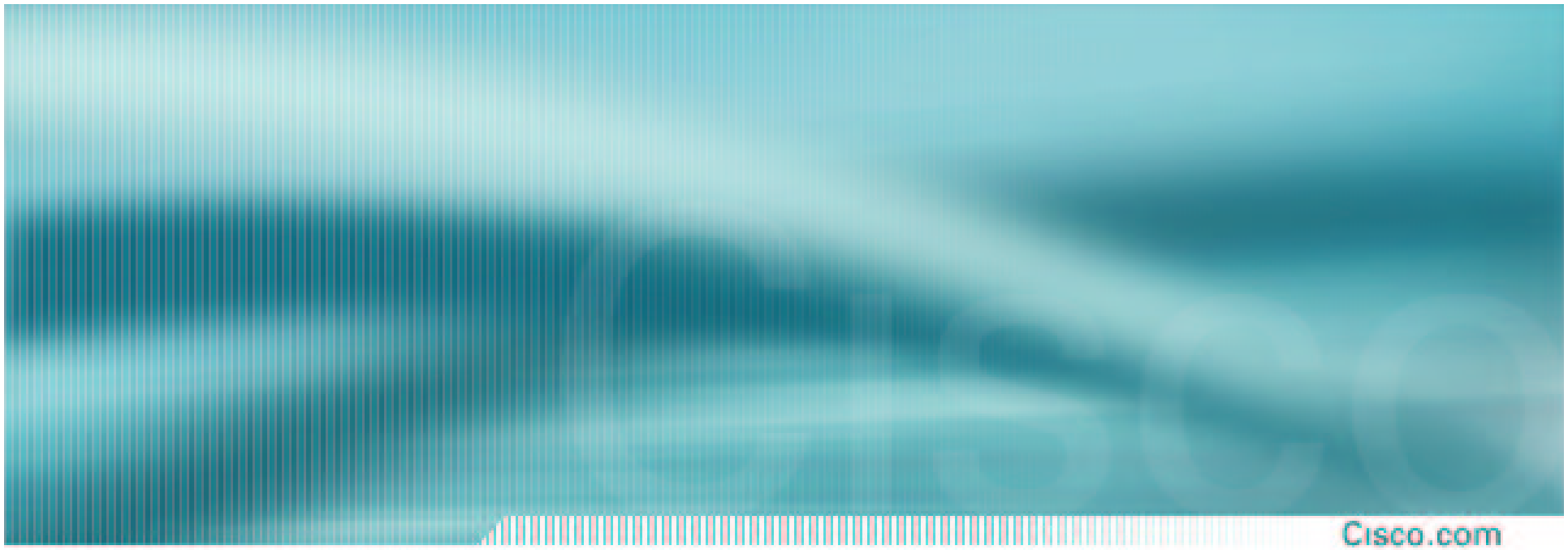


1.- Políticas de Seguridad

Qué es una Política de Seguridad?

Es mucho más que sólo comprar un Firewall

- Qué bienes necesito proteger?
- Qué servicios pleneo ofrecer?
- Qué riegos de seguridad crea eso?
- Qué herramientas o métodos están disponibles para reducir mis riesgos de seguridad?
- Cúal es mi “nivel aceptable de riesgo?”



2.- Identidad

Identidad - Authentication, Authorization, and Accounting (AAA)

Herramienta para control de red y acceso a sistemas

- **Authentication**

  Verifica identidad—
  Quién eres?

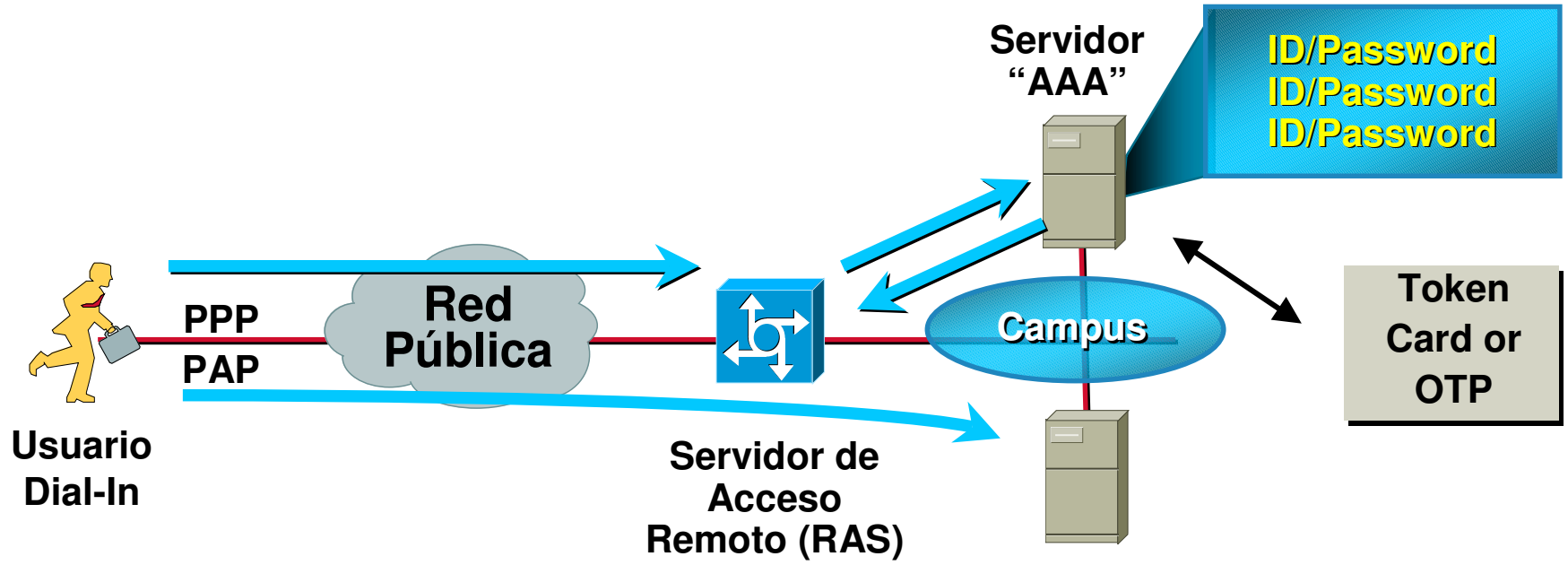
- **Authorization**

  Configura integridad—
  Qué esta permitido que haga?

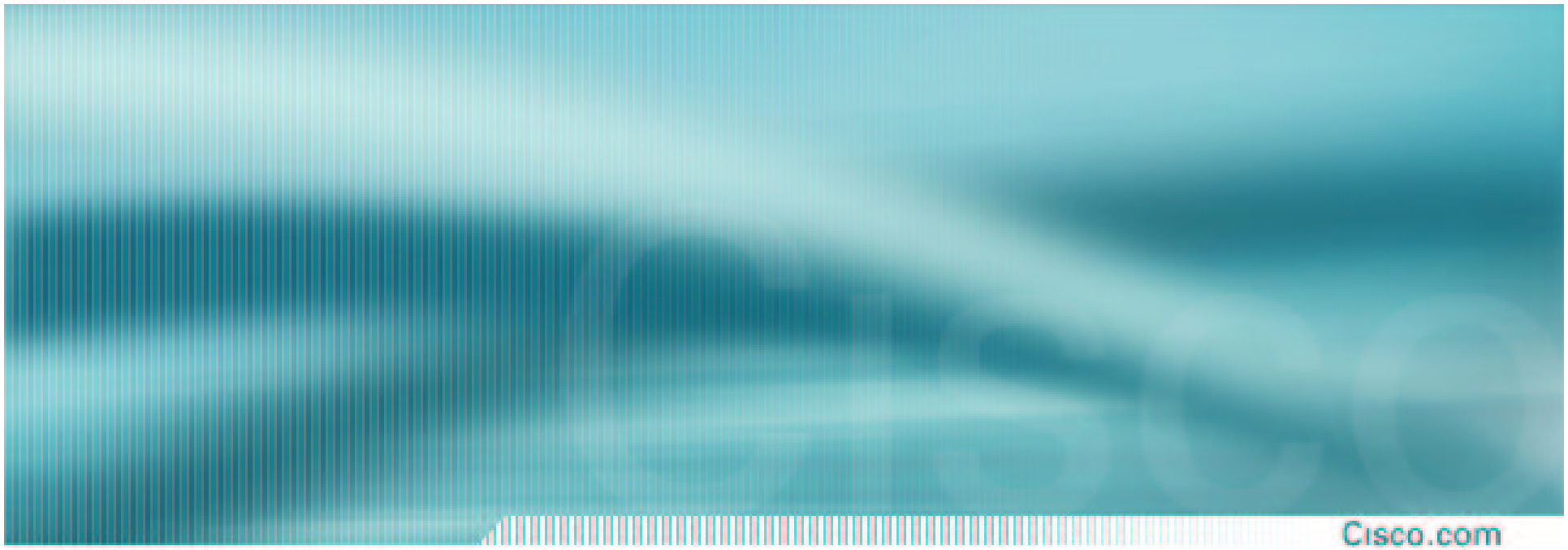
- **Accounting**

  Asiste con auditoria—
  Qué hizó?

Identidad - Authentication, Authorization, Accounting (AAA) - Proceso



- Usuario ingresa con password al RAS
- RAS envía ID/password a Srvidor "AAA"
- Server "AAA" autentifica ID/password del usuario e indica al RAS aceptar (o no aceptar)
- RAS acepta (o no acepta) la llamada



3.- Seguridad Perimetral

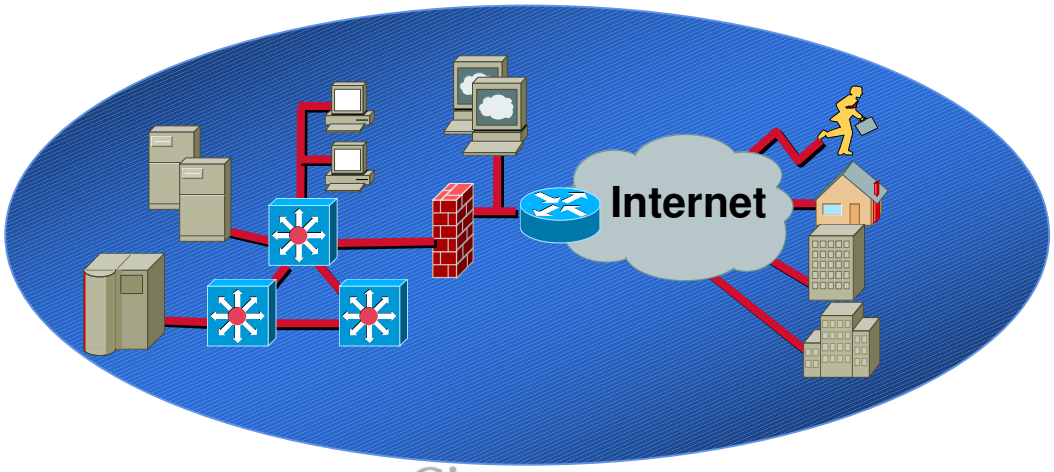
Seguridad Perimetral

- Reglas de firewall en núcleo de infraestructura
- Amplio range en tipo de firewall appliances
- Firewall personales en clientes VPN
- Escalabilidad de Firewall más alla de Gigabit Ethernet

Firewall Appliances

ACLs

CAR



Firewalls Integrados

Firewalls: Personal Integrado Appliances

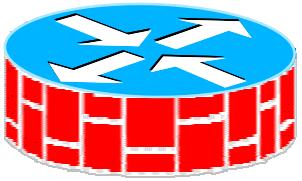
El Firewall

- **Permite acceso seguro a los recursos**
- **Proteje la Red de:**
  - **Intrusiones no autorizadas desde fuentes externas e internas**
  - **Ataques Denial-of-Service (DOS)**

Elección de Firewall

- **Basado en Router**

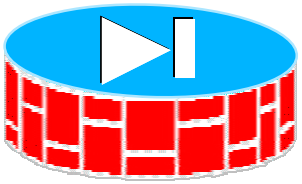
  Integrado OS vs. Pareja de OS y aplicaciones

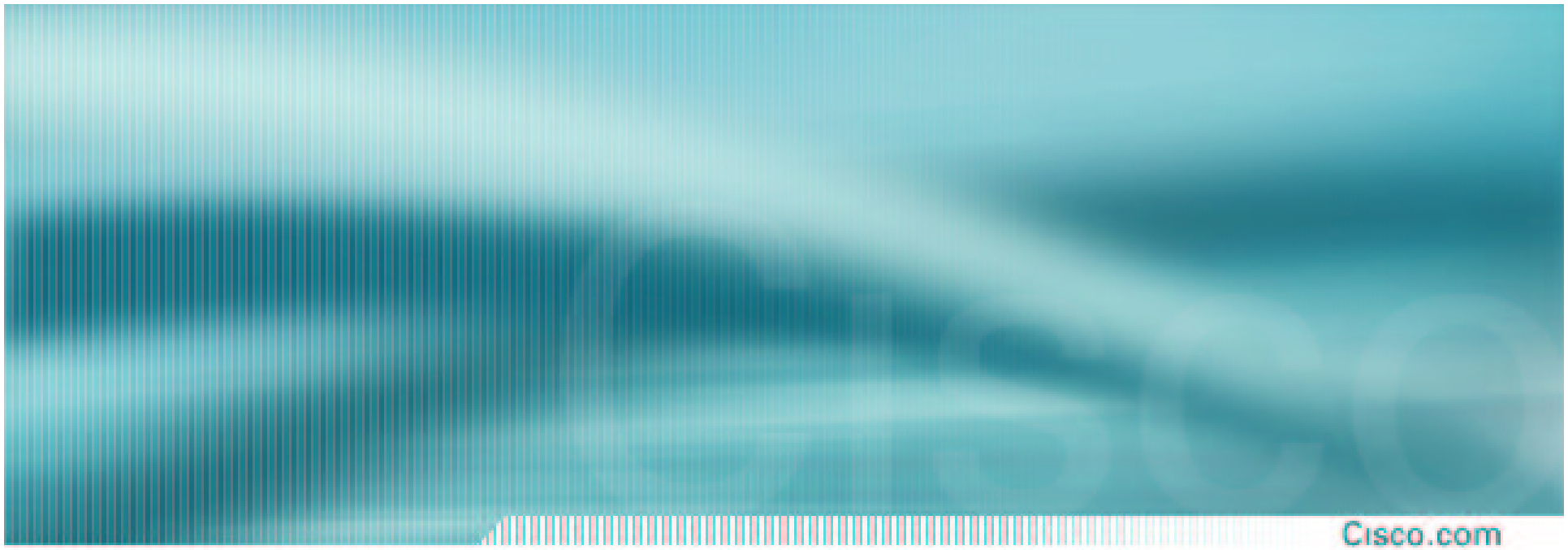


- **Appliance vs. software**

  OS propio, seguro

  Filtraje de Paquetes vs. Proxy





4.- Conectividad Segura

Conectividad Segura

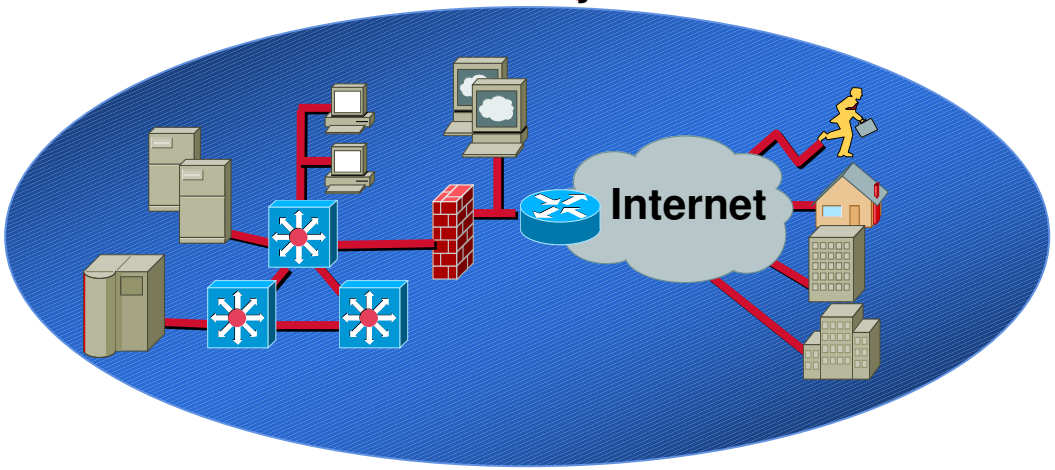
- Accesos Remotos VPN a gran escala
- Encriptación integrada en infraestructura de red
- Wireless VPN

Firewall Appliances

Concentradores y Routers VPN

VPN

Host-to-Host



Clientes VPN

Firewall Appliances

Concentradores VPN

Routers optimizados para VPN

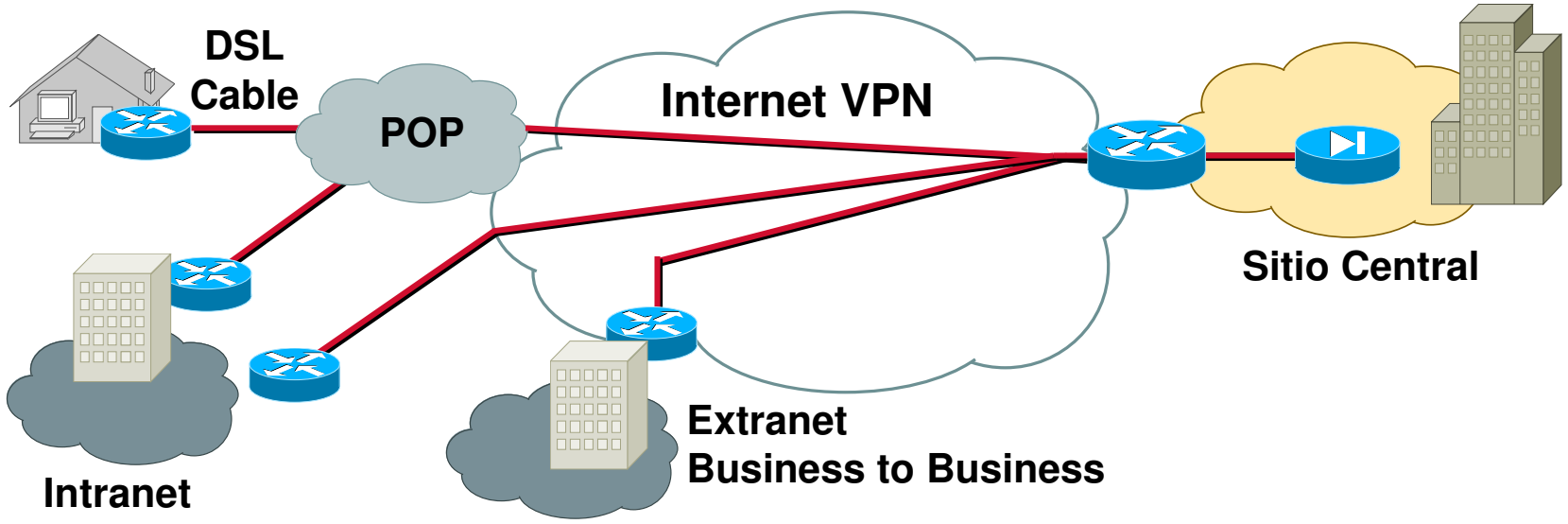
VPN´s Site-to-Site

Sitio Remoto - Access CPE
(Customer Premise Equipment)

Sitio Central - Corporación

VPN Router/Firewall
Firewall

VPN Router/Firewall
Firewall



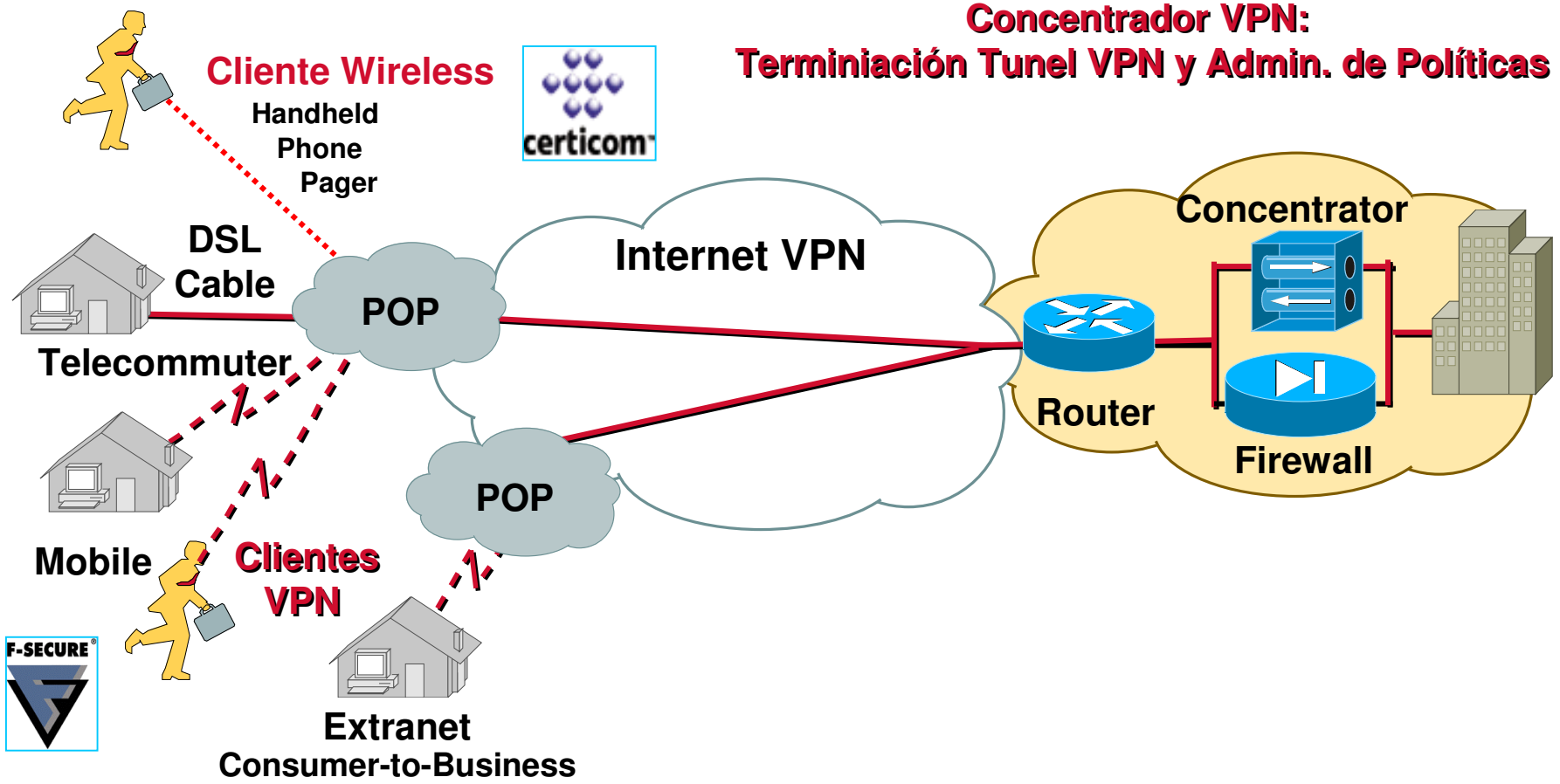
- **Servicios VPN en software IOS de routers**

VPN´s – Accesos Remotos

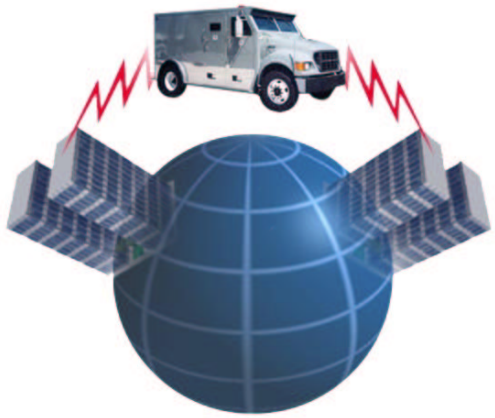
Acceso Remoto Cliente

Sitio Central - Corporación

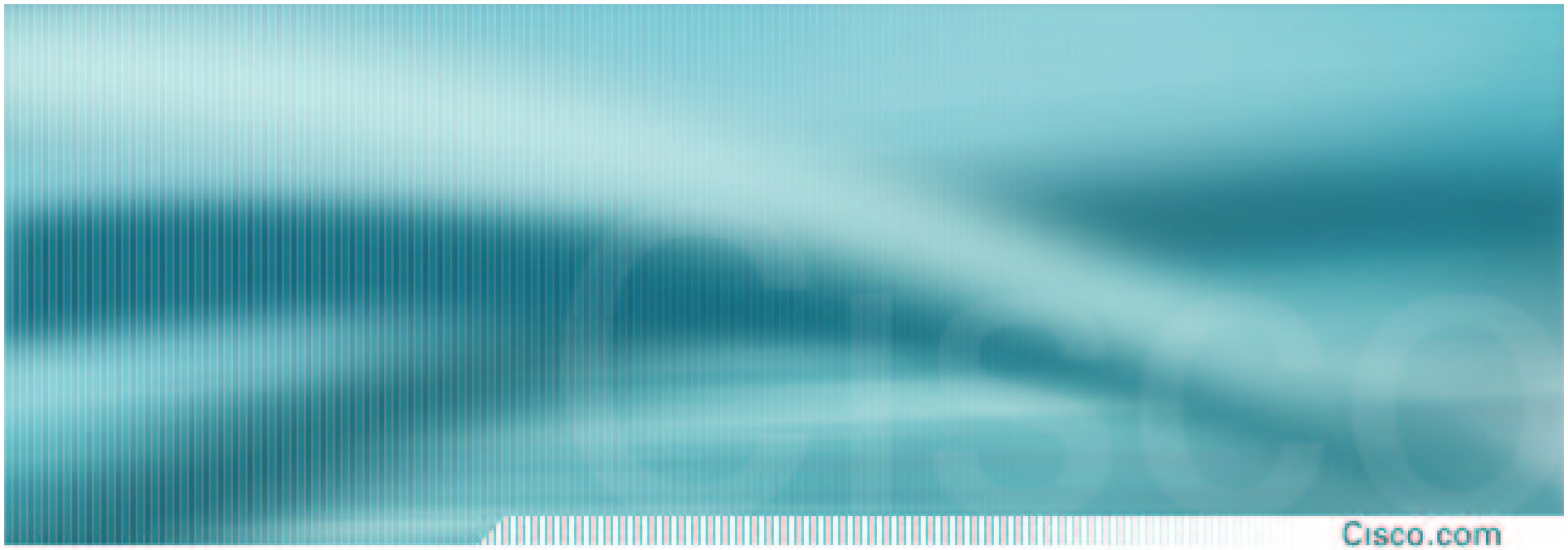
Router WAN
Firewall
Concentrador VPN:
Terminiación Tunel VPN y Admin. de Políticas



Encriptación



- **Algoritmo de dato cifrado en un formato inteligente**
- **Cada sesión requiere un proceso**
  - **Estabiliza asociación segura**
  - **Determina e intercambia llaves (keys) cifradas**
- **IPSec**
  - **Proceso Automatizado y estándarizado**
  - **IP Nativo—puesto en cualquier lugar!**
  - **Perfecto para VPNs!**
  - **DES/56 bit, 3DES/168 bit**
  - **Intercambio de llaves (Keys) (tiempo real, automatizado)**

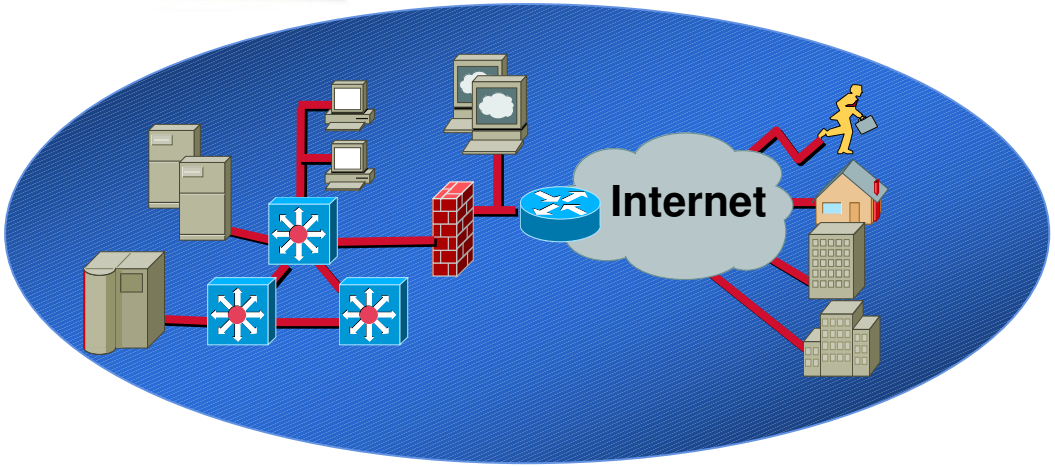


5.- Monitoreo de Seguridad

Monitoreo de Seguridad

- IDS Integrado en infraestructura de red
- Amplio rango de IDS appliances
- Fuerte vulnerabilidad en scanning software
- Monitoreo en vínculo al host y aplicaciones

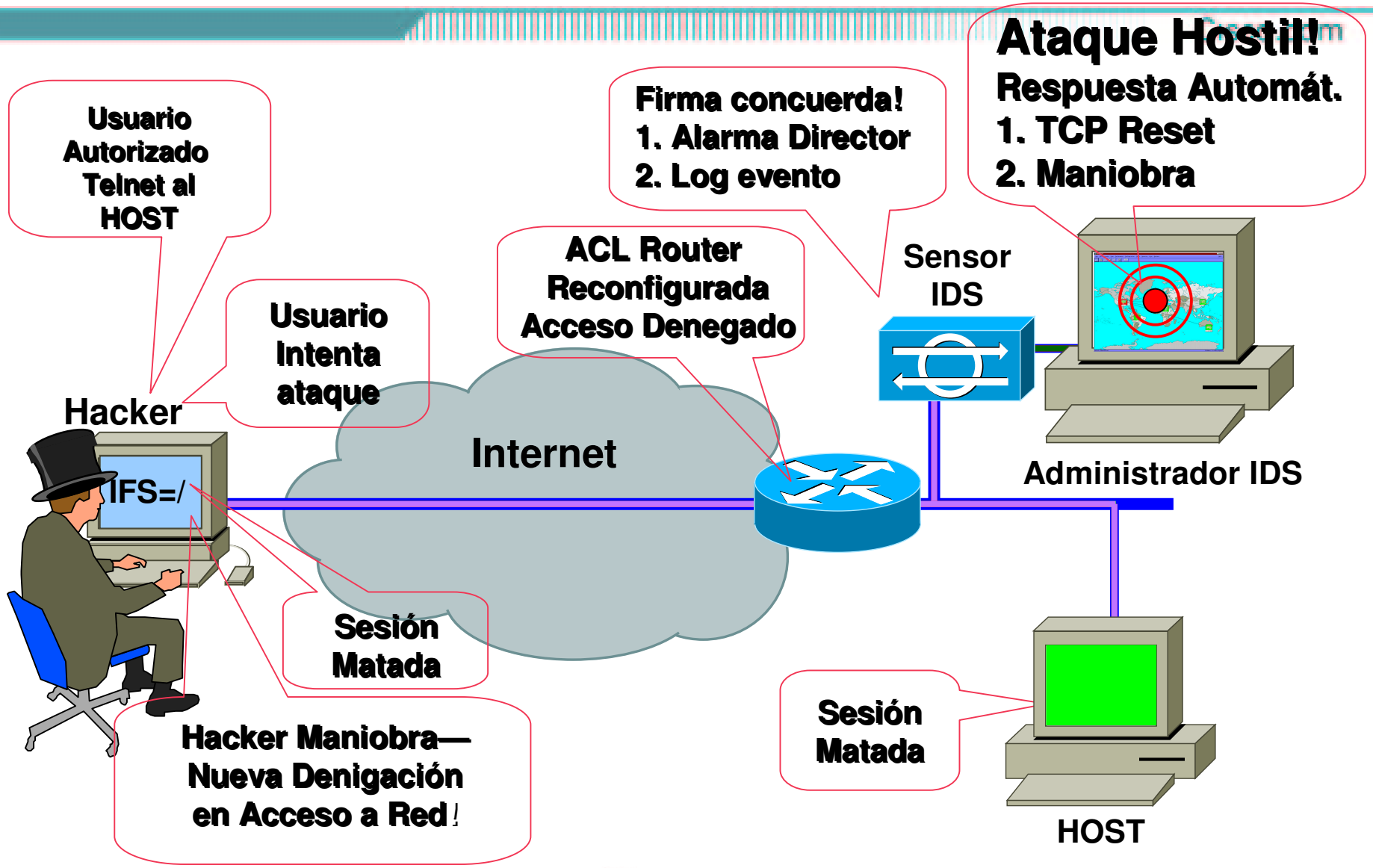
IDS Appliances



IDS Integrado
IDS
Scan de
Vulnerabilidad

IDS Appliances
IDS Integrado

Detección de Intrusos
Sensando la Red



Detección de Instrusos Lugar

- **Perimetral**

  Appliance

- **DMZ**

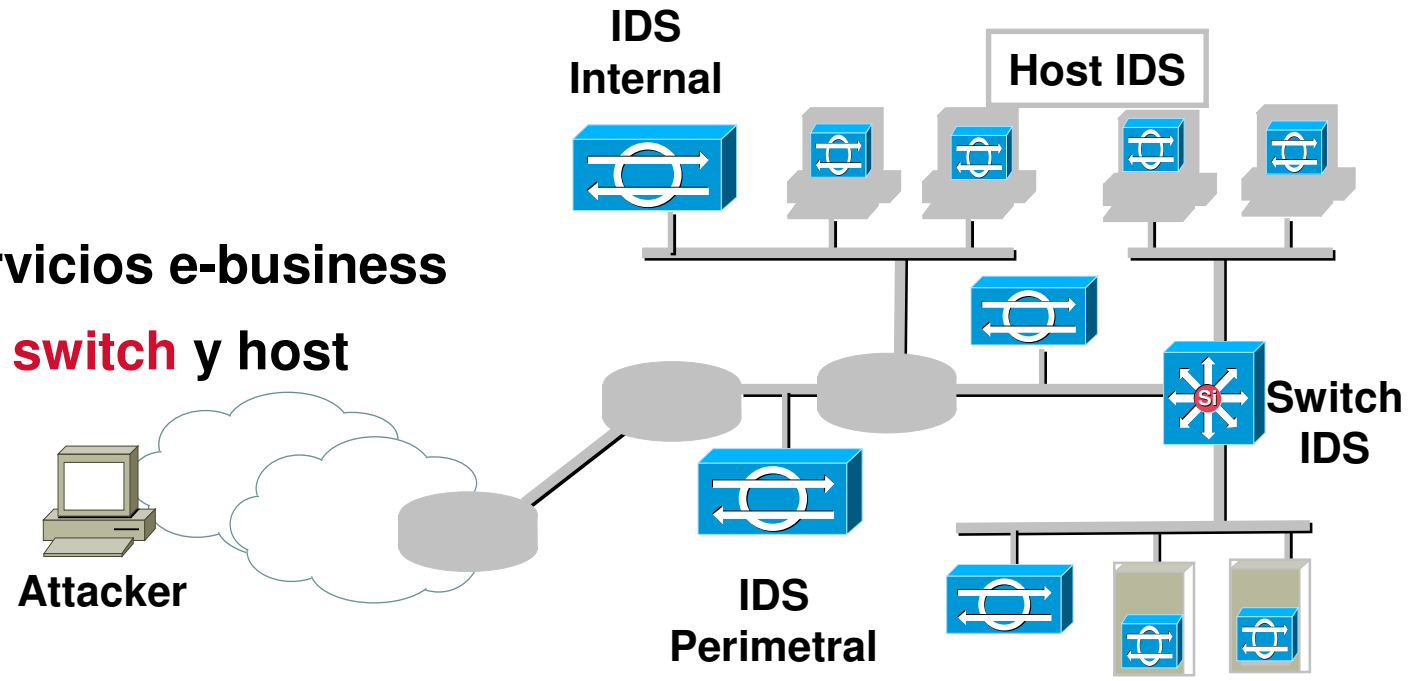
  Proteje servicios e-business

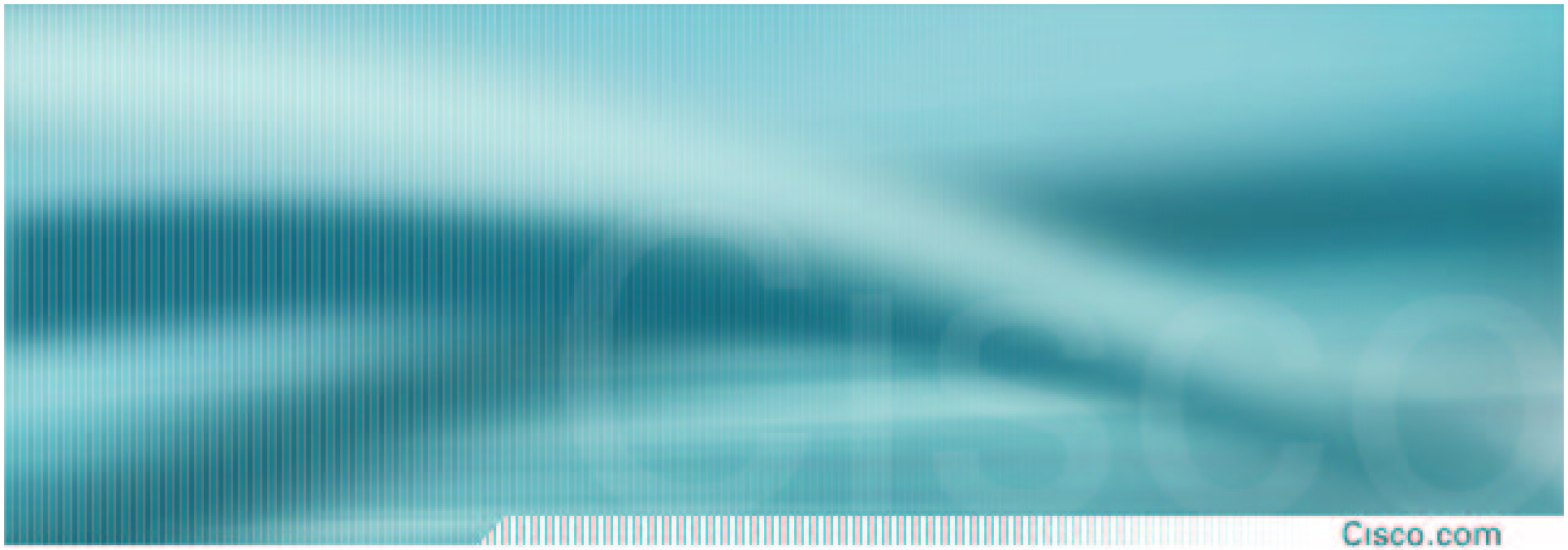
  Appliance, switch y host

- **Internal**

  Areas con altas pérdidas financieras y bajo esfuerzo en seguridad!

  Appliance, switch y host

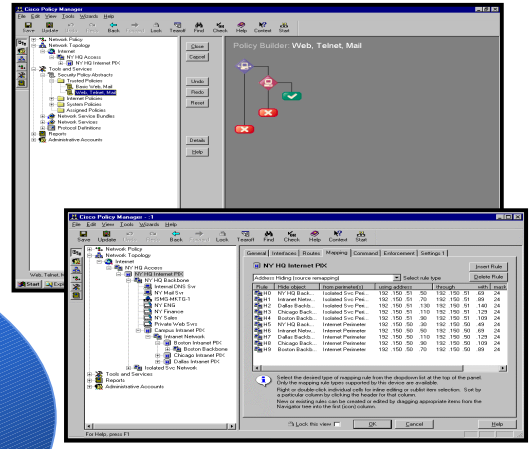




6.- Administración de Seguridad

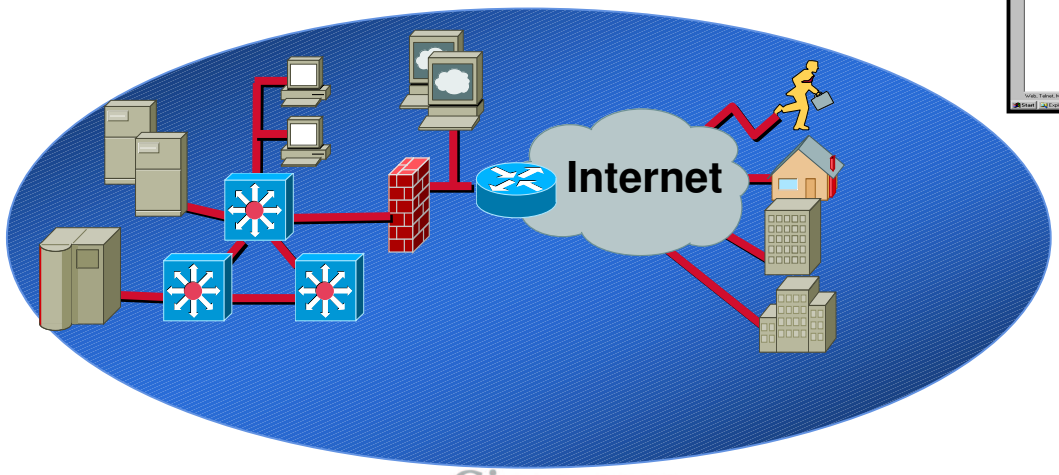
Administración de Seguridad

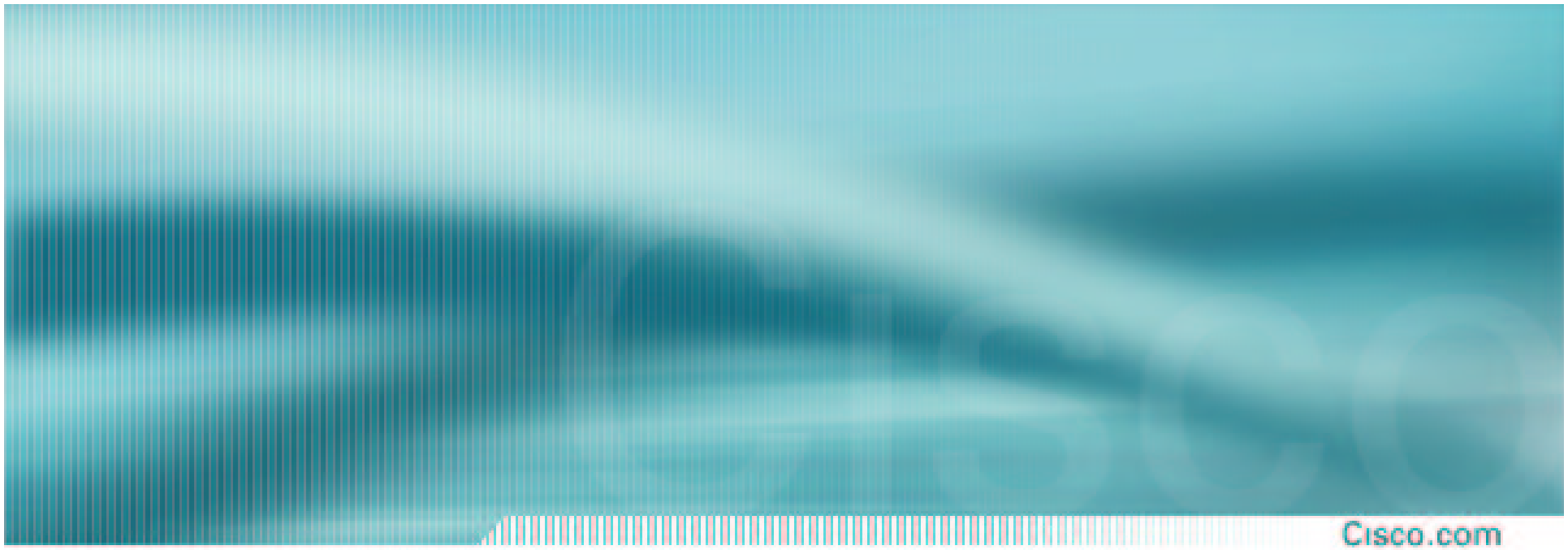
- Administración de Seguridad Centralizada para las Corporaciones
- Integración con sistemas administración de red central y servicios de directorios
- Administradores de dispositivos para sistemas individuales
- APIs abiertas para administración de partners (Ecosistema)



Administración de Seguridad Consolidada

- Dispositivos
- Políticas
- Usuarios





Tecnologías para Seguridad

Componentes para una Red Segura

Cisco.com

Conectividad Segura	Seguridad Perimetral	Monitoreo de Seguridad	Identidad	Administración de Seguridad

VPN

- Cisco VPN Concentrators
- Cisco PIX™ Firewalls

Firewalls

- Cisco PIX™ Firewalls

Detección de Intrusos Scanning

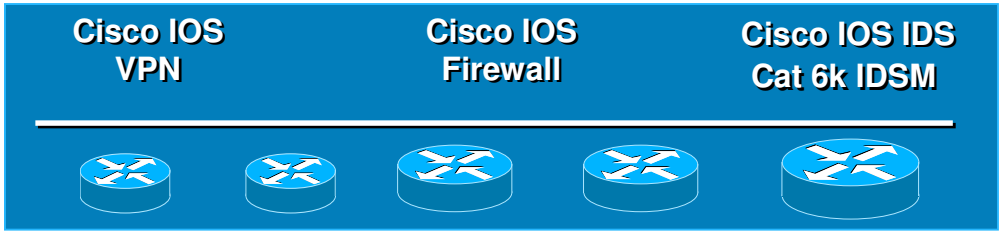
- Cisco IDS Appliances

Autenticación

- Cisco Access Control Server (ACS)

Políticas

- CiscoWorks VPN Mgmt Solution
- Cisco Secure Policy Manager (CSPM)
- Web Device Managers

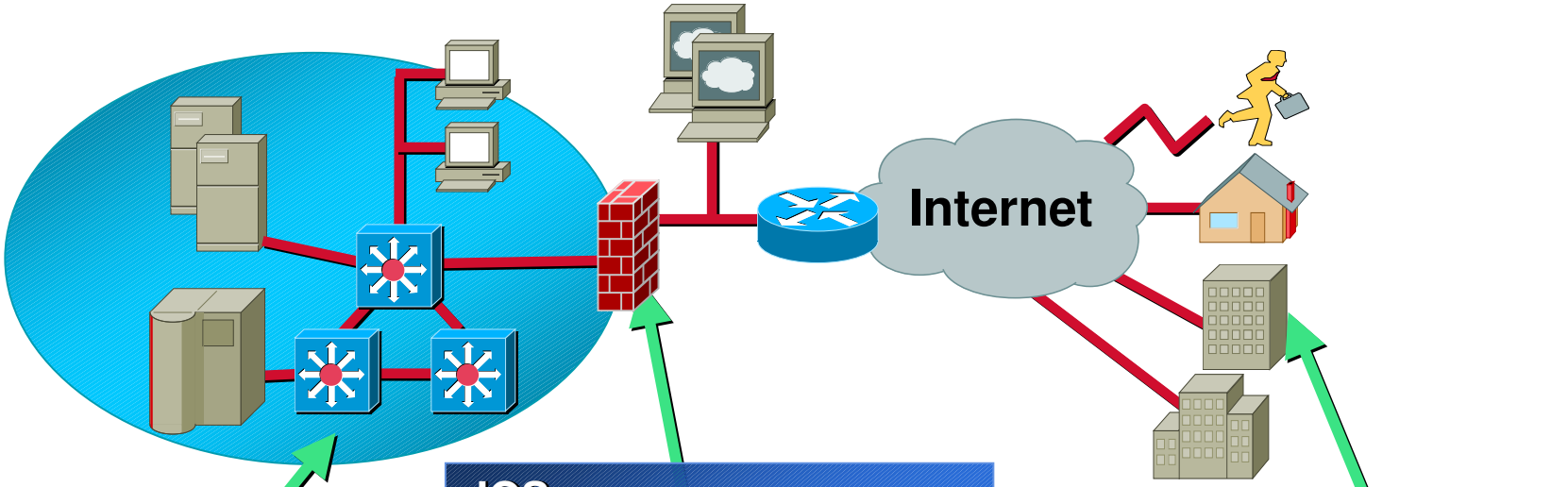


Tecnologías para Seguridad

Campus

Perímetro

Sitios Remotos

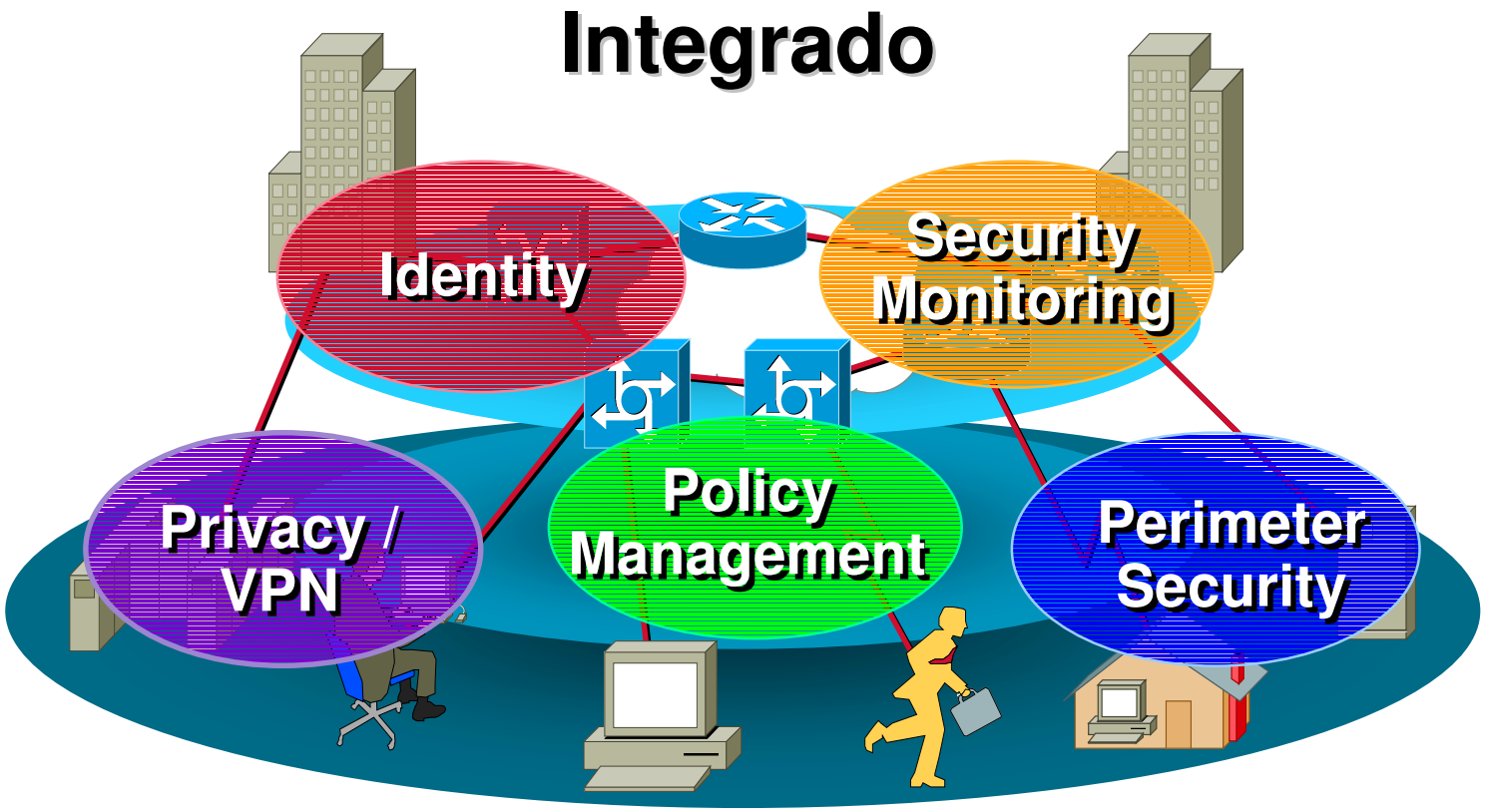


- Catalyst 6500 Switch
  - VLAN
  - Private VLAN
  - IDS Line Card
  - IOS Firewall
- Cisco Secure Policy Manager / CSPM

- IOS
- PIX Firewall 525/535
- VPN 3000 Concentrator Series
- IDS 4220/4230
- 71xx/72xx/75xx Routers
- Cisco Secure ACS

- PIX Firewall 501,506, 515
- IDS 4210
- VPN 3000 Client
- 17xx/26xx/36xx Routers

Resumen



Sumario

- La Seguridad es un sistema en la Red
- Seguridad en Red es más que Firewalls
- Un buen Sistema de Administración más Defensa en Profundidad es igual a Seguridad en Red

En Conclusión…

La Seguridad esta en la Red

- Personas
- Procesos
- Productos

} = Seguridad de Red


Cisco Systems